Protecting What You Thought Was Yours: Expanding Employee Privacy to Protect the Attorney-Client Privilege from Employer Computer Monitoring

KARA R. WILLIAMS*

I. INTRODUCTION

Ashlee has been working at her current job for almost two years, and she was confident that she understood her privacy rights as an employee of the company.[1] However, she was completely unaware that one day, by sending a private e-mail to her private attorney from her work computer, she might have jeopardized the confidentiality of her conversations that had occurred in what she thought was strict confidence.[2]

Recently, Ashlee had been experiencing some problems with her supervisor at work, and she feared that his conduct might be amounting to sexual harassment. Concerned about her safety and her job, Ashlee sought the advice of a private attorney, who instructed her to keep him informed of the conduct of her employer. One day at work, Ashlee's employer made a lewd remark to her about her body and the outfit she was wearing. Upset by this comment, Ashlee quickly went back to her office and e-mailed her private attorney from her work-provided computer, giving him a great deal of personal information, as well as information about her employer's conduct. In response, her attorney concluded that Ashlee had an actionable claim for sexual harassment, and Ashlee subsequently filed suit against her employer.

Despite the private nature of the conversation, during discovery for the pending lawsuit, Ashlee's employer demanded the production of Ashlee's confidential e-mail exchange with her personal attorney. Although this

---

* Articles Editor, *Ohio State Law Journal*; J.D., The Ohio State University Moritz College of Law, expected 2008. B.A., University of Rochester, 2005. I would like to thank Professor L. Camille Hébert for introducing this topic and providing me with helpful guidance and suggestions throughout the writing process. I would also like to thank my parents, Bob and Sherry Williams, for their love, support, and endless encouragement. A special thanks to Andrew and Renee for being there for me every day and supporting me in everything I do.

[1] "Ashlee" and her accompanying story is a hypothetical situation described to set up the issue that has occurred in recent cases, to which this Note is addressed.

[2] *See* L. CAMILLE HÉBERT, EMPLOYEE PRIVACY LAW § 8A:33.50, at 376 (Supp. 2006) (discussing a new development in the law regarding "[c]laims of waiver of attorney-client privilege to electronic communications by present and former employees").

communication between Ashlee and her attorney appears to be a confidential communication protected by the attorney-client privilege, it is not that simple. In actuality, the employer, like most employers, had a policy of monitoring its employees' computer use, and the policy provided that the employer could monitor e-mail communications at any time.[3] In addition, Ashlee had signed an acknowledgement and receipt of this monitoring policy when she began working for her employer. The employer claims that, as a result, Ashlee has waived her attorney-client privilege because she has, in effect, disclosed the communication to a third party—the employer.[4]

However, Ashlee's response is that, although there is a monitoring policy in place, her employer has never before actually monitored employees' communication. As a result, she claims that she had a reasonable expectation of privacy in her private e-mail communications with her attorney and thus they should be protected by the attorney-client privilege.[5] The court in this dispute is left with the difficult and novel question of what effect employer-monitoring has on confidential communications between an employee and his or her private attorney that would otherwise be protected by the attorney-client privilege.[6] It is this problem that will be addressed in this Note.

Over the past fifteen years, there has been a "technological revolution" in the workplace as businesses throughout the country have increasingly turned to computer technology as the primary tool to communicate, conduct research, and store information.[7] A majority of contemporary employment settings provide employees with access to e-mail and the Internet.[8] The most

---

[3] In today's business world, employer monitoring of employee computer use is extremely common. *See* Kesan, *infra* note 15 at 291 (discussing the substantial number of employers who currently monitor their employees' computer and e-mail use).

[4] These facts are a variation on the facts of Curto v. Medical World Communications, Inc., No. 03CV6327(DRH)(MLO), 2006 WL 1318387, at *1–2. (E.D.N.Y. May 15, 2006).

[5] *See id.* at *3–4 (discussing whether actual enforcement of computer monitoring policy should be a factor to consider in the expectation of privacy and waiver of privilege analysis).

[6] This is a new issue that has recently emerged in several cases within the past few years. *See infra* Part IV for a discussion on the recent cases addressing this issue.

[7] U.S. GEN. ACCOUNTING OFFICE, EMPLOYEE PRIVACY: COMPUTER USE MONITORING PRACTICES AND POLICIES OF SELECTED COMPANIES, 02-717, at 1 (September 2002), *available at* http://www.gao.gov/new.items/d02717.pdf.

[8] *Id.* at 4 (reporting that as of September 2001, sixty-five million of the 115 million employed adults age twenty-five and over, almost fifty-seven percent, used a computer at work). This data is from a study conducted by the U.S. General Accounting Office (GAO) on computer use and monitoring in the workplace. *Id.* at 2. The GAO conducted its study by reviewing literature of research on private and public sector monitoring of employees' use of e-mail, the Internet, and computer files. *Id.* at 2. Additionally, the GAO interviewed privacy experts from universities, officials and researchers from

common use for a computer at work is to access the Internet or use e-mail, and the percentage of employees using the Internet or e-mail at work grew from about eighteen percent in 1998 to almost forty-two percent in 2001.[9] Computer and Internet use has continued to rise; in October 2003, seventy-seven million people reported using a computer at work, and approximately seventy-five percent of those seventy-seven million reported that they used the computer to browse the Internet or check e-mail.[10]

"As the use of these electronic technologies has increased in the workplace, so have employers' concerns about their employees' use of company-owned computing systems" such as the Internet and e-mail "for activities other than company business."[11] It is no secret that many people use their work computers for personal use. A recent study estimated that sixty-one percent of employees who utilize a work-owned Internet connection admitted that they spend at least some time surfing non-work-related websites during the work day.[12] For these employees, approximately twenty-four percent of their time spent accessing the Internet at work was found to be non-work-related.[13] As the use of technology in the workplace increases (and as the potential for abuse also increases), employers are using

---

national business organizations, and conducted interviews with officials from fourteen Fortune 1,000 private sector companies from five industry categories. *Id.*

[9] *Id.* at 4.

[10] U.S. Dep't of Labor, *Computer and Internet Use at Work Summary*, BUREAU OF LABOR STATISTICS (Aug. 10, 2005), *available at* http://www.bls.gov/news.release/ciuaw.nr0.htm. The seventy-seven million workers using a computer on the job in 2003 was an increase from sixty-five million in 2001. *Id.*

[11] GAO, *supra* note 7, at 4.

[12] Lexis Nexis Press Release, January 24, 2007, http://www.lexisnexis.com/media/press-release.aspx?id=0946.asp (last visited Apr. 20, 2008). *See also* Vivian Marino, *Personal Business: Diary; Confessions of Workers at Play on the Computer*, N.Y. TIMES, July 15, 2001, § 3, at 10 (confirming "what is already known," a technology-and-ethics survey in 2001 found that among the 1,130 people it surveyed, two of three admitted that they were guilty of at least one case of "technology abuse"—i.e., using a work computer for personal use—within the past year, while eighty-four percent had witnessed such a transgression by a co-worker).

[13] Websense, Inc., 2006 *Web@Work* Survey, http://www.websense.com/global/en/PressRoom/PressReleases/PressReleaseDetail/?Release=0605171215 (last visited Apr. 20, 2008) (finding that of those employees who access non-work-related websites, the average time spent accessing the Internet at work is 12.81 hours per week, and the average time accessing non-work related websites at work is 3.06 hours per week). *See also* Vivian Marino, *supra* note 12.

technology themselves to engage in monitoring and surveillance of their employees.[14]

Employers' monitoring of their employees' computer use is extremely common in American businesses. One commentator indicates that at least seventy-seven percent of large American businesses monitor electronic communications that are transmitted through the workplace.[15] Moreover, the amount of information that can be obtained by an employer through computer monitoring of employees is "staggering."[16] While the technological aspects of monitoring are beyond the scope of this Note, in general these products have tremendous capabilities to monitor employees, such as showing the online activities of employees, including websites visited and for how long, as well as allowing employers to monitor the use of chat rooms, programs run, files used, and e-mail sent and received.[17]

Given how widespread employee monitoring appears to be, privacy advocates have raised concerns about the potential for employers to infringe

---

[14] L. CAMILLE HÉBERT, EMPLOYEE PRIVACY LAW § 8A:1, at 5 (2006) (noting that "[a]n increasingly common method of electronic monitoring chosen by employers is monitoring of the work of employees through computers").

[15] Jay P. Kesan, *Cyber-working or Cyber-shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 291 (2002). For other reports on the prevalence of employer monitoring of computer use, *see, e.g.*, American Management Association and the E-Policy Institute, *2005 Electronic Monitoring & Surveillance Survey*, http://www.amanet.org/research/pdfs/EMS_summary 05.pdf (last visited Apr. 20, 2008) (reporting a study based on 526 companies found that as many as seventy-six percent of employers now monitor their employees' computer use); Carl S. Kaplan, *Reconsidering the Privacy of Office Computers*, N.Y. TIMES ON-LINE, July 27, 2001, http://www.nytimes.com/2001/07/27/technology/27CYBERLAW.html (finding that "up to 14 million U.S. workers are subject to contin[ual] surveillance of their e-mail and Internet use" while at work); American Management Association, *2003 E-mail Rules Policies, and Practice Survey*, http://www.amanet.org/research/pdfs/E-mail_Policies_Practices.pdf (last visited Apr. 20, 2008) (reporting that more than fifty percent of over 1000 companies monitor employee e-mail).

[16] HÉBERT, *supra* note 14, § 8A:1, at 6. Most relevant to this Note, among the products developed that can obtain such "staggering" amounts of information are computer software products that have been developed to monitor employees' use of the Internet and employer networks. *Id.*

[17] *See* Rosemary Orthmann, *Software Enables Employers to Monitor Employees' Internet Use*, EMP. TESTING L. & POL'Y REP., Apr. 1998, at. 55. *See also* Gail Lasprogata, Nancy J. King & Sukanya Pillay, *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada*, 2004 STAN. TECH. L. REV. 4, 20–21 (2004) (reporting that software enables employers to "monitor employees' use of chat rooms, programs run, games played, files used, bytes transferred or downloaded, time spent downloading, and e-mail sent and received").

upon employees' right to privacy.[18] It is true that many employers have "developed policies to notify their employees that they monitor use of these systems and to provide guidance to employees about the appropriate uses of computing technologies."[19] However, although many companies announce their monitoring policies ahead of time, it nevertheless appears that employer monitoring continues to raise many questions about employees' rights to their privacy.

While an employer's motivation to monitor its employees' computer use may be completely legitimate,[20] the methods used by employers to achieve these ends may raise significant privacy issues, to the extent that employers are monitoring more than simply work activity. By its nature, monitoring of employees' computer use is likely to stray—either intentionally or unintentionally—into the realm of private employee activity.[21] The use of electronic monitoring by government employers may violate the Fourth Amendment rights of employees to be free from unreasonable searches and seizures.[22] In addition, several cases have been brought by employees claiming a violation of common-law restrictions on electronic monitoring; these employees have argued that monitoring constitutes a tort of invasion of privacy.[23] As employers continue to monitor their employees, it seems likely that these types of privacy suits will continue.

In addition to the potential for the traditional constitutional and common law violations of privacy by employer monitoring, there is a new concern for the privacy of employees in the technological revolution. It is clear that employees' use of work-provided computers for personal communications is

---

[18] GAO, *supra* note 7, at 4 (claiming that "privacy advocates have raised concerns about the potential for employers to infringe upon employees' right to privacy").

[19] *Id.*

[20] HÉBERT, *supra* note 14, § 8A:2, at 19 (stating that employers have a right to reasonably protect themselves from employee theft and other employee misconduct).

[21] *Id.* For example, an employer monitoring Internet use for the legitimate purpose of assessing productivity may unintentionally discover a personal e-mail communication that would be considered private employee activity, rather than work-related computer use.

[22] *Id.* at § 8A:4, 28. The U.S. Supreme Court announced in *O'Connor v. Ortega* that manual searches by government employers can implicate the Fourth Amendment when the areas searched are areas in which employees have a reasonable expectation of privacy. *Id.*

[23] *Id.* at § 8A:6, 52. *See, e.g.*, Kelleher v. City of Reading, No. Civ.A.01-3386, 2002 WL 1067442, at *1 (E.D. Pa. May 29, 2002) (plaintiff-employee claimed invasion of privacy when employer accessed employee's e-mail); Smyth v. Pillsbury Co., 914 F. Supp. 97, 100 (E.D. Pa. 1996) (plaintiff-employee claiming invasion of privacy based on an employer's monitoring of employee's e-mail); TGB Insurance Services Corp. v. Superior Court, 96 Cal. App. 4th 443, 447 (Cal. Ct. App. 2002) (plaintiff-employee claimed privacy interest in a computer provided by his employer for his use at home).

commonplace in today's business world.[24] One such personal communication that may occur is when an employee communicates with his attorney via e-mail on a work-provided computer. Under other circumstances, this communication would usually be protected by the attorney-client privilege.[25] However, an emerging issue is how courts will interpret the scope of attorney-client privilege as it relates to e-mails exchanged on employer-issued computers that are subject to employer monitoring.[26] "At stake when an attorney and client communicate [via e-mail] . . . is whether the communication originated in confidence and whether the parties to the communication have maintained its confidentiality."[27] The crucial question for employee privacy has become whether workplace monitoring by an employer may either prevent the employee's e-mail communication with his attorney from being confidential or may constitute a waiver of the privilege.[28]

Part II of this Note will discuss the traditional cases dealing with an employee's right to privacy in the workplace. Beginning with the U.S. Supreme Court case *O'Connor v. Ortega*,[29] this section will discuss the

---

[24] *See* Lexis Nexis, *supra* note 12 (reporting the increase in computer usage at work, the article states that "nearly three of four (73% [of]) office workers are either as or more likely to use the Internet at work for personal reasons than they were two years ago; sixty-eight percent are as or more likely to send or receive personal emails on their work accounts"). *See also* Dion Messer, *To: Client@Workplace.com: Privilege at Risk?*, 23 J. MARSHALL J. COMPUTER & INFO. L. 75, 77 (2004) (discussing a national survey conducted by the executive director of the E-Policy Institute, which indicates that an overwhelming ninety percent of employees surveyed nationwide use e-mail at work for personal business). Moreover, as technology expands, companies are beginning to allow their employees to work remotely; according to one survey, eighty-one percent of hiring managers have policies in place that allow employees to work remotely (including working from home or from a satellite office). *See* Andrew R. Hickey, *A Remote Worker Can Threaten Network Security*, SEARCHNETWORKING.COM, Oct. 11, 2006, http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci1222867,00.html. The increasing number of employees working from outside of the office also leads to the inference that employees will use these work-provided computers for personal communications.

[25] *See* PAUL R. RICE, THE ATTORNEY-CLIENT PRIVILEGE IN THE UNITED STATES § 2:2 at 10 (2d ed. 1999) (stating that when the proponent of the attorney-client privilege has presented sufficient facts to satisfy each element of the privilege, the communications between the attorney and client will be protected, and this protection is absolute).

[26] *See* Kelcey Nichols, *Hiding Evidence From the Boss: Attorney-Client Privilege and Company Computers*, 3 SHIDLER J. L. COM. & TECH. 6, 6 (2006).

[27] Thomas H. Watkins & Kevin L. Leahy, *Avoiding Malpractice at the Speed of Light: Are Your Email Communications Protected and Secure?*, 68 TEX. B.J. 579, 579 (2005).

[28] *See* discussion *infra* Parts III, IV, V.

[29] O'Connor v. Ortega, 480 U.S. 709 (1987).

traditional rule governing employees' privacy, namely, whether the employee had a reasonable expectation of privacy. In Part III, the basic elements of the attorney-client privilege will be discussed. Communicating via e-mail over a work computer has the potential to disturb two elements of the privilege: the requirement of keeping the communication in confidence and the possibility of waiving the privilege. Part IV will discuss the new line of employee privacy cases that deal with the issue of an employee communicating with his private attorney via e-mail over a work-provided computer. Three cases have followed the traditional analysis of the expectation of privacy cases to determine whether the privilege still exists. However, one case has held that the expectation of privacy cases are not controlling in this new context of attorney-client communications. Part IV will also discuss the reasons the court gives for distinguishing the two sets of cases.

Finally, Part V proposes a possible new approach to looking at the employee privacy cases dealing with the attorney-client privilege. First, it is argued that the attorney-client privilege should be protected. Second, the Note suggests possible solutions to protect the attorney-client privilege for an e-mail sent by an employee, even though his employer may have been monitoring his computer usage. It is proposed that this issue could be handled by following the novel analysis set forth by the U.S. District Court for the Eastern District of New York in *Curto v. Medical World Communications, Inc.*,[30] through legislative action such as an amendment to the Electronic Communications Privacy Act (ECPA),[31] through enacting state legislation, or by the ABA issuing an opinion requiring attorneys to exercise caution with their clients when communicating via e-mail.

II. TRADITIONAL PRIVACY IN THE WORKPLACE AND AN EMPLOYEE'S REASONABLE EXPECTATION OF PRIVACY

The use of e-mail and the Internet in the workplace has significantly expanded in the last several years, and, as a result, employers are feeling the need to monitor their employees' use of these devices. There are many legitimate reasons why employers might want to monitor their employees' use of e-mail and the Internet.[32] To the extent that employer use of electronic

---

[30] No. 03CV6327(DRH)(MLO), 2006 WL 1318387 (E.D.N.Y. May 15, 2006).

[31] 18 U.S.C. §§ 2510–22, 2701–11 (2000).

[32] HÉBERT, *supra* note 14, § 8A:2, at 17. Some employers engage in electronic monitoring as an objective means of evaluating the work performance of employees and to provide employees with feedback on their performance. *Id.* at 18. More common justifications employers give for monitoring employees include preventing employee theft and the disclosure of confidential information or intellectual property. *Id.*; *see also*

monitoring actually measures work activity of employees, rather than personal or private activity, the privacy implications are relatively minor.[33] However, even electronic monitoring that is aimed at recording work activity may result in the recording of personal, non-work activity by employees.[34] Therefore, although employers may see the monitoring of employee use of e-mail and the Internet as an effective way to maintain control over the workplace, this type of monitoring may create legal pitfalls in the form of privacy invasion.[35]

A right of privacy is recognized under both the common law[36] and the Fourth Amendment to the United States Constitution.[37] In both situations, the aggrieved party must show a reasonable expectation of privacy.[38] In order for a workplace intrusion to constitute a "search or seizure" under the Fourth Amendment, there must be an intrusion into an individual's "actual (subjective) expectation of privacy" and that expectation of privacy must be "one that society is prepared to recognize as 'reasonable.'"[39] Similarly, one claiming an "intrusion on seclusion," the common law right to privacy violation, must show, *inter alia*, a subjective expectation of privacy and that

---

FREDERICK S. LANE III, THE NAKED EMPLOYEE: HOW TECHNOLOGY IS COMPROMISING WORKPLACE PRIVACY 12 (2003) (noting that one of the most important justifications given by employers of monitoring employees is minimizing theft and sabotage by employees). In addition, monitoring employees is justified because improper, non job-related use of the Internet and use of e-mail for personal messages cause a decrease in employee productivity, and personal messages of an offensive nature can expose employers to liability for harassment or discrimination. Louise A. Fernandez, *Privacy in the Workplace*, 696 PRACTISING L. INST., LITIG. & ADMIN. PRAC. COURSE HANDBOOK SERIES 275, 278 (Oct.–Nov. 2003).

[33] HÉBERT, *supra* note 14, § 8A:2, at 17.

[34] *Id.*

[35] Fernandez, *supra* note 32, at 278.

[36] *See* RESTATEMENT (SECOND) OF TORTS § 652B (1997) (discussing the tort of "intrusion upon seclusion").

[37] U.S. CONST. amend. IV. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.* Because this Note deals with the implications of the Fourth Amendment right to privacy, it applies only to employees working for state actors, as that is the only category of workers protected by the Amendment.

[38] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740 (1979) ("[T]he application of the Fourth Amendment depends on whether the person invoking its protection can claim a . . . 'reasonable . . . expectation of privacy' that has been invaded by government action."); Kline v. Sec. Guards, Inc., 386 F.3d 246, 260 (3d Cir. 2004) (plaintiff asserting cause of action for invasion of privacy under Restatement (Second) of Torts § 652B must show a "reasonable expectation of privacy").

[39] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

the expectation is objectively reasonable.[40] The U.S. Supreme Court first applied Fourth Amendment principles to employee privacy in its landmark case of *O'Connor v. Ortega*, where it made clear that manual searches by government employers can implicate the Fourth Amendment when the areas searched are areas in which employees have a reasonable expectation of privacy.[41] While *Ortega* dealt with personal effects found in an employee's office, the same principles have been expanded to deal with employees' expectations of privacy in computer files and e-mail.

A. *The Supreme Court's Seminal Case:* O'Connor v. Ortega

In *Ortega*, a state hospital commenced an investigation into suspected improprieties by its chief of professional education (Ortega); in the course of the investigation, hospital personnel searched Ortega's office without his knowledge or consent.[42] In the search, the hospital personnel found evidence that was subsequently used to impeach the credibility of a witness testifying on Ortega's behalf and private patient billing information.[43] After its investigation of the alleged improprieties, the hospital fired Ortega.[44] Following his discharge, Ortega commenced a federal action alleging that the search of his office violated the Fourth Amendment.[45]

The Supreme Court held that although some hospital personnel may have had a legitimate right of access to his office, Ortega had a reasonable expectation of privacy in his desk and file cabinets.[46] The Supreme Court emphasized that an employee's expectation of privacy in his office, desk, and files "may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."[47] However, in this case, "there was no evidence that the Hospital had established any reasonable regulation or policy discouraging employees such as Dr. Ortega from storing personal papers and effects in their desks or file cabinets . . . although the absence of such a

---

[40] *See* Medical Lab. Mgmt. Consultants v. Am. Broad. Cos., 306 F.3d 806, 812–13 (9th Cir. 2002) (stating that to prevail, the plaintiff must show "(a) an actual, subjective expectation of seclusion or solitude in the place, conversation, or matter, and (b) that the expectation was objectively reasonable").

[41] O'Connor v. Ortega, 480 U.S. 709 (1987).

[42] *Id.* at 713.

[43] *Id.*

[44] *Id.* at 712–713.

[45] *Id* at 714.

[46] *Id.* at 718–719 (finding a reasonable expectation of privacy in this area because Ortega did not share his desk and file cabinets with other employees, he had occupied the same office for seventeen years, and he kept personal items and records in his office).

[47] *O'Connor*, 480 U.S. at 717.

policy does not create an expectation of privacy where it would not otherwise exist."[48] Importantly, the Court stated that "[g]iven the great variety of work environments . . . the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis."[49]

B. *Beyond* Ortega*: An Employee's Expectation of Privacy in Computer Files and E-mails*

Although *Ortega* dealt with personal effects found in desks and file cabinets, the same considerations that the Supreme Court espoused in *Ortega* have been adopted to measure an employee's expectation of privacy in his computer files and e-mail.[50] In general, to measure an employee's expectation of privacy in computer files and e-mail, courts generally consider four factors: (1) whether his employer maintains a policy banning personal or other objectionable use,[51] (2) whether the company monitors the use of the employee's computer or e-mail, (3) whether third parties have a right of access to the computer or e-mails,[52] and (4) whether the employer notified the employee, or whether the employee was aware of the use and monitoring policies.[53] Several courts have applied these four factors to determine whether an employee's privacy rights had been violated by an employer's monitoring of e-mail and Internet use.

In *United States v. Simons*, the U.S. Court of Appeals for the Fourth Circuit addressed the issue of whether a government employee has a

---

[48] *Id.* at 719.

[49] *Id.* at 718.

[50] *See* Muick v. Glenayre Elec., 280 F.3d 741, 743 (7th Cir. 2002); Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000); Thygeson v. U.S. Bancorp, No. CV-03-467, 2004 WL 2066746, at *20 (D. Or. Sept. 15, 2004).

[51] The Electronic Communications Privacy Act of 1986 (ECPA) generally prohibits unauthorized access to or retrieval of a wire or electronic communication while it is in electronic storage or transit. *See* 18 U.S.C. §§ 2510–22, 2701–11 (2000). However, consent is a defense to a claim under these statutes; if one of the parties to the communication has given consent to its interception, there has been no violation of the Act. *See id.* Therefore, it is relevant whether the employer maintains a policy banning non-work related use of the Internet and whether the employee is aware of such policy.

[52] An employee may take precautions to limit access; for example, computers can be password-protected, and e-mails can be encrypted.

[53] *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005) (discussing the four factors generally applied by courts when analyzing an employee's expectation of privacy).

reasonable expectation of privacy with respect to his use of the Internet.[54] In addressing the reasonableness of the defendant's expectations of privacy in his Internet use, the court noted that the employer had a policy restricting Internet use to official business use and indicating that audits of Internet use would be conducted.[55] In light of this policy, the court held that the defendant could have no reasonable expectation of privacy with respect to his Internet use, and therefore that no Fourth Amendment violation had occurred.[56] The court found that Simons could not have a reasonable expectation of privacy in files downloaded from the Internet in light of the existence of the policy, as any subjective expectation of Simons that his Internet use would remain private "was not objectively reasonable after [his employer] notified him that it would be overseeing his Internet use."[57]

Several courts have also found that employees have no reasonable expectation of privacy in e-mail that is sent over a work computer.[58] In *Smyth v. Pillsbury Co.*, the Eastern District of Pennsylvania held that there was no reasonable expectation of privacy in e-mail an employee sent to a supervisor over the company e-mail system, even though the employer made assurances that such communications would not be intercepted by management or used as grounds for reprimands.[59] The court found that "[o]nce [the] plaintiff communicated the alleged unprofessional comments to a second person . . . over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost."[60]

---

[54] United States v. Simons, 206 F.3d 392, 398–99 (4th Cir. 2000). In *Simons*, the employee was an electronic engineer employed by the CIA who had access to the Internet through a government-provided computer network. *Id.* at 395. The systems analyst discovered the defendant had downloaded pornographic material from the Internet to his work computer. *See id.* at 396.

[55] *Id.* at 395–96.

[56] *Id.* at 399–401.

[57] *Id.* at 398–99.

[58] *See* Smyth v. Pillsbury Co., 914 F. Supp. 97, 100–101 (E.D. Pa. 1996). *See also* Bohach v. Reno, 932 F. Supp. 1232, 1234–35 (D. Nev. 1996) (holding that employees did not have objectively reasonable expectations of privacy in electronic communications on the employer's computer network); United States v. Monroe, 50 M.J. 550, 558 (A.F. Ct. Crim. App. 1999) (finding that the accused could have no objectively reasonable expectation of privacy in the e-mail system maintained by the government because that system was stated to be "for official business only" and notice was given that the "system was subject to monitoring"); McClaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *4–5 (Tex. Ct. App. May 28, 1999) (finding that even though plaintiff created a personal password for his e-mail account, plaintiff still did not have a reasonable expectation of privacy in the contents of the e-mail messages he sent over his work computer).

[59] Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996).

[60] *Id.*

However, other courts have found that public sector employees do have an objectively reasonable expectation of privacy that their e-mail messages will not be routinely accessed.[61] In *United States v. Slanina*, the U.S. Court of Appeals for the Fifth Circuit held that an employee had a reasonable expectation of privacy in his computer files where the computer was maintained in a closed, locked office, the employee had installed passwords to limit access, and the employer "did not disseminate any policy that prevented the storage of personal information on city computers and also did not inform its employees that computer usage and Internet access would be monitored."[62] Similarly, the U.S. District Court for the District of Kansas found that an employee had a reasonable expectation of privacy in private computer files, despite a warning that there shall be no expectation of privacy in using the employer's computer system.[63] A reasonable expectation of privacy was found because employees were allowed to use computers for private communications, were advised that unauthorized access to users' e-mail was prohibited, were given passwords to prevent access by others, and no evidence was offered to show that the employer ever monitored private files or employee e-mails.[64]

It is clear that balancing the four factors, courts have come out with different results on employees' claims of privacy violations, both under the Fourth Amendment and common law. Although the courts are mixed, to the extent that employer computer monitoring reveals non-work-related information about an employee, a court may find an intrusion upon objectively reasonable expectations of privacy sufficient to implicate the protections of the Fourth Amendment against unreasonable searches and seizures.[65]

III. THE ATTORNEY-CLIENT PRIVILEGE AND THE PROBLEMS PRESENTED BY E-MAIL COMMUNICATIONS BY COMPUTER-MONITORED EMPLOYEES

A. *The Growing Use of E-mail for Attorney-Client Communications*

E-mail, with its speed of communication and ease of access, has become an essential tool in today's business world, and law firms are among the businesses increasingly turning to e-mail to communicate. One of the most

---

[61] *See, e.g.*, United States v. Slanina, 283 F.3d 670, 676–77 (5th Cir. 2002); Haynes v. Office of the Attorney Gen. Phil Kline, et al., 298 F. Supp. 2d 1154, 1161–62 (D. Kan. 2003).

[62] *Slanina*, 283 F.3d at 676–77.

[63] *Haynes*, 298 F. Supp. 2d at 1161–62.

[64] *Id.*

[65] HÉBERT, *supra* note 14, § 8A:6, at 52.

efficient means for attorneys to communicate with clients is via e-mail, and e-mail is increasingly replacing phone calls as the preferred method of communication between attorneys and clients.[66] Moreover, attorneys have endorsed e-mail technology, and the American Bar Association (ABA) has approved this method of communication as well.[67] The use of e-mail among attorneys is widespread; a 2002 survey revealed that eighty percent of attorneys use e-mail one or more times per day, and an additional eleven percent use e-mail one to four times per week.[68] Clearly, e-mail is a vital part of many attorneys' legal communications.

However, the use of e-mail communications between attorneys and clients poses new problems in today's technological business world. Complex privacy and confidentiality issues arise because e-mail communications between attorneys and clients may end up in the clients' employers' hands due to the growing phenomenon of workplace monitoring of employees' computer use.[69] Problems of confidentiality in the context of attorney-client e-mails are becoming a serious issue for attorneys and clients, as personal use of computers at work is widespread.[70] As employees increasingly use e-mail at work for personal communications, it is likely that an employee involved in a legal dispute will use e-mail to communicate with his attorney about the ongoing issues. Given the prevalence of employers

---

[66] Messer, *supra* note 24, at 75.

[67] ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99–413 (1999), *available at* http://www.abanet.org/cpr/fo99-413.html (discussing the subject of protecting the confidentiality of unencrypted e-mails). The ABA responded to varied state opinions on the use of e-mail for attorney-client communications by adopting its official position of a full endorsement of the use of ordinary e-mail for professional legal communication:

> A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct . . . because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail.

Id.

[68] Kathryn A. Thompson, *Technology Snapshot: The Results are In*, ABA LEGAL TECHNOLOGY RESOURCE CENTER (Apr. 4, 2003), http://www.lawtechnology.org/presentations/techshow2003/techshow2003_files/frame.htm (slide 25) (additionally finding that only three percent of attorneys reported never using e-mail to communicate with clients).

[69] Messer, *supra* note 24, at 76.

[70] *See supra* Part I (discussing the high instance of employees using their work computers for personal use).

monitoring the computer use of employees,[71] the issue has arisen as to the effect of workplace monitoring on the attorney-client privilege that might otherwise protect the confidential communications.

B. *The Attorney-Client Privilege: What is it?*

The attorney-client privilege is an evidentiary rule that is designed to encourage the free flow of information between an attorney and his or her client by protecting that information by keeping the communications confidential.[72] However, the mere fact that an individual communicates with an attorney does not make his communications privileged.[73] Before a communication from a client to an attorney may qualify for the attorney-client privilege, it must satisfy a number of elements. Generally, most jurisdictions follow the common law of privilege, and many courts follow a variation of Professor Wigmore's eight elements that must be met for a communication to be privileged. Professor Wigmore's attorney-client privilege consists of:

> (1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived.[74]

This is closely mirrored by Proposed Federal Rule of Evidence 503(b), which, although never adopted, is frequently cited with approval.[75]

---

[71] *See supra* Part I (discussing the prevalence of workplace monitoring of employee computer use).

[72] ATTORNEY-CLIENT PRIVILEGE IN CIVIL LITIGATION: PROTECTING AND DEFENDING CONFIDENTIALITY 2 (Vincent S. Walkowiak ed., American Bar Association 3d ed. 2004) (1993). "The underlying assumption is that our legal system is more civilized and efficient because we recognize the attorney-client privilege." *Id.*

[73] RICE, *supra* note 25, § 2:1 at 6. *See also* United States v. Costanzo, 625 F.2d 465, 468 (1980) ("[I]t is true that '[a] communication is not privileged simply because it is made by or to a person that happens to be a lawyer.'")

[74] RICE, *supra* note 25, § 2:1 at 8.

[75] *Id.* at 8–9. Proposed Federal Rule 503(b) provides:

> (b) General rule of privilege. A client has a privilege to refuse to disclose and to prevent any other person from disclosing confidential communications made for the purpose of facilitating the rendition of professional legal services to the client, (1) between himself or his representative, (2) between his lawyer and the lawyer's representative, (3) by him or his lawyer to a lawyer representing another in a matter of common interest, (4) between representatives of the client or between the client and a representative of the client, or (5) between lawyers representing the client.

Accordingly, one of the central requirements of the attorney-client privilege is that the communication must be made confidentially.[76] An important component of the confidentiality requirement is that the communication may not be subsequently disclosed, as disclosure to a third party generally constitutes a waiver of the privilege.[77]

When the proponent of the privilege has presented sufficient facts to satisfy each element, the communications between the attorney and client will be protected. Assuming a limited number of exceptions (including waiver of the privilege) are not applicable,[78] this protection is absolute.[79] "It is believed that the protection must be absolute in order to further the privilege's end—encouraging candor and full disclosure by the client."[80] Therefore, if all elements of the privilege are met, the privilege precludes the disclosure of the communications regardless of the need that could be demonstrated for the information in them.[81]

C. *The Problems Threatening the Attorney-Client Privilege When an Employee Communicates with His or Her Attorney Through E-Mail on a Work Computer*

When an attorney and client communicate through e-mail over the Internet, two elements of the attorney-client privilege are at stake: whether the communication originated in confidence and whether the parties to the communication have maintained its confidentiality.[82] If a communication fails to meet either of these two elements, it will not be protected by the attorney-client privilege.[83]

Id. at 9–10.

[76] Nichols, *supra* note 26, at 6.

[77] *Id.* at 10.

[78] Other exceptions to the attorney-client privilege include the crime/fraud exception, the joint client exception, exceptions for actions by individuals to whom a fiduciary duty is owed, the will contest exception, and the open or public meeting exception (Sunshine Laws). *See generally* RICE, *supra* note 24, § 8, at 7–139.

[79] RICE, *supra* note 25 § 2:2, at 10.

[80] *Id.* § 2:2, at 10–11. If the protection were not absolute, the protection would not be predictable; in response the client could not rely on it and the client's full disclosure might be "chilled." ATTORNEY-CLIENT PRIVILEGE, *supra* note 72, at 2.

[81] RICE, *supra* note 25 § 2:2, at 11.

[82] Watkins, *supra* note 27, at 579. The second element, "whether the parties to the communication have maintained its confidentiality" constitutes a waiver of the privilege.

[83] *See* RICE, *supra* note 25 § 2:1, at 8.

1. *Lack of Confidentiality to Make Out a Prima Facie Case of Privilege*

For the attorney-client privilege to attach to a communication, "a communication must be made in confidence of the relationship and under circumstances from which it may reasonably be presumed that it will remain in confidence."[84] The attorney-client privilege maintains a strict confidentiality requirement, and two elements must be met for the communication to originate in confidence.[85] The first is a subjective element; the client must intend his communications with his attorney be confidential.[86] The second is an objective element; the client's subjective intention of confidentiality must be reasonable under the circumstances.[87] The subjective and objective elements are closely related factual questions, and so are often determined by courts using similar factors.[88]

Therefore, in order to qualify as privileged, there must be a reasonable expectation of privacy in e-mail communications.[89] If there is no reasonable expectation of privacy in the communication, then it will not be confidential and no privilege will attach in the first place.[90] It is a hallmark of the attorney-client privilege that "'[t]he moment the confidence ceases' . . . 'privilege ceases.'"[91] If there are third parties present during the communication, the communication is not confidential unless those third

---

[84] Wilcoxon v. United States, 231 F.2d 384, 386 (10th Cir. 1956), *cert. denied*, 351 U.S. 943 (1956). *See also, e.g.*, United States v. Schwimmer, 892 F.2d 237, 244 (2d Cir. 1989) (holding that the attorney-client privilege "requires a showing that the communication in question was given in confidence and that the client reasonably understood it to be so given"); United States v. Melvin, 650 F.2d 641, 645 (5th Cir. 1981) ("A communication is protected by the attorney-client privilege . . . if it is intended to remain confidential . . . and understood to be confidential.").

[85] RICE, *supra* note 25, § 2:1, at 7.

[86] *Id.*

[87] *Id.* § 6:1 at 8.

[88] *Id.* The most important of these factors is the circumstances surrounding the communication. *Id.* at 8–9.

[89] Lucy Schlauch Leonard, Comment, *The High-Tech Legal Practice: Attorney-Client Communications and the Internet*, 69 U. COLO. L. REV. 851, 863 (1998).

[90] *See id.* at 864 ("[T]he privilege does not apply to the situation where it is the intention or understanding of the client that the communication is to be made known to others.") (quoting *In re* Grand Jury Proceedings, 727 F.2d 1352, 1358 (4th Cir. 1984)).

[91] United States v. Tellier, 255 F.2d 441, 447 (2d Cir. 1958) (holding that a communication between an attorney and a client is not confidential when the expectation was that the substance of the conversation would be transmitted by the attorney to a third party).

parties are necessary to the communication.[92] This creates a potential danger for the confidentiality requirement if clients communicate with their attorneys via e-mail while on a work computer that is being monitored.[93] If the employer's monitoring of employees' e-mail use means the employer is "present" during the communication (because they are monitoring the content of the e-mail) and the employer is not a necessary party to the communication (which they often will not be in an employee's private legal dispute), then the communication will not be "confidential" and therefore will not be protected by the privilege.[94]

In addition, the attorney-client privilege does not apply if the client understands that the information will be made known to third parties.[95] Therefore, if the employer has a policy of monitoring its employees and the employee is aware of the policy, the attorney-client privilege may not apply because the employee "understand[s] . . . that the communication is to be made known to others."[96]

When dealing with whether an employee understands that the communication will be made known to others, the Electronic Communications Privacy Act of 1986 ("ECPA") is important.[97] The ECPA generally provides legal protection for intercepted e-mail.[98] The ECPA makes the interception of an e-mail message by a third party a criminal act and protects the privilege afforded any illegally intercepted message; an individual violates the statute if he or she "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to

---

[92] Leonard, *supra* note 89, at 863. *See also* United States v. Schwimmer, 892 F.2d 237, 237 (2d Cir. 1989) (holding that the attorney-client privilege extends to communications with an accountant assisting an attorney in defense of the client where the attorney directed the client to speak freely with the accountant); United States v. Evans, 954 F. Supp. 165, 170 (N.D. Ill. 1997) (holding there could be no privilege for communications between an attorney and client when an attorney friend of the client was also present); State v. Colton, 384 A.2d 343, 345–46 (Conn. 1977) (finding there could be no attorney-client privilege in a conversation between a witness and an investigator when a third party representing the defendant was also present).

[93] Leonard, *supra* note 89, at 862 (suggesting that the issue of whether the communication was made in confidence presents potential problems for e-mail and attorney-client privilege).

[94] This danger to the confidentiality requirement is particularly imminent where the dispute is not one involving the employer, as it is less likely that the employer will be perceived as a necessary party to the communication.

[95] *See In re* Grand Jury Proceedings, 727 F.2d 1352, 1356 (4th Cir. 1984) (finding that the privilege does not apply to the situation "where it is the intention or understanding of the client that the communication is to be made known to others").

[96] *Id.* at 1356.

[97] *See* 18 U.S.C. §§ 2510–2522 (2000).

[98] *See generally* 18 U.S.C. § 2511 (2000).

intercept, any wire, oral, or electronic communication."[99] Thus, an attorney can usually rely on the ECPA to protect the attorney-client privilege of illegally intercepted e-mail.[100]

However, workplace monitoring often falls under an exception to the statute, as an employer may legally monitor employees' e-mail and Internet use if it obtains the prior consent of the employee.[101] When an employee signs an employment agreement that allows his employer to own and monitor e-mail, he may be giving up the statutory privacy protection afforded to him under the ECPA.[102] Under these circumstances, employer interception of the e-mail is no longer "in accordance with" or "in violation of" the ECPA, and the communication may lose the immunity from discovery afforded by § 2517(4).[103] Therefore, if the employee is aware of his employer's computer monitoring policy, that knowledge could prevent the communication from originating in confidence, and the attorney-client privilege would not apply.[104]

Other commentators who have discussed the attorney-client privilege in the context of e-mail and the Internet are also skeptical about the existence of privacy expectations.[105] This skepticism is fueled by security problems with

---

[99] 18 U.S.C. § 2511(1)(a) (2000).

[100] *See* Messer, *supra* note 24, at 91. This statutory protection is outlined in 18 U.S.C. § 2515 (2007), titled "Prohibition of use as evidence of intercepted wire or oral communications," which provides that "no part of the contents of such communication and no evidence derived therefrom may be received in evidence."

[101] 18 U.S.C. § 2511(2)(d)(2007) ("It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception . . . ."). Courts will uphold the consent defense if the employee's consent is found to be either express or implied. *See* Mark J. Manta, *Electronic Surveillance and Employee Privacy in the Workplace*, METROPOLITAN CORP. COUNS., June 1996, *available at* www.theelawfirm.com/articles.php ("The ECPA allows the interception of electronic communications where one of the parties to the communication has given prior consent, express or implied, to such an interception.").

[102] Messer, *supra* note 24 at *92. *See also* Kevin J. Baum, Comment, *E-Mail in the Workplace and the Right of Privacy*, 42 VILL. L. REV. 1011, 1027 (1997) ("By proving implied consent through a well-disseminated e-mail policy, the likelihood of an employer's liability is decreased.").

[103] *See* 18 U.S.C. § 2517(4) (2000).

[104] Some courts treat consent to employer monitoring under the ECPA as a waiver of the attorney-client privilege, rather than from preventing the communication from being confidential in the first place. Under either analysis, the ECPA would not protect an employee's attorney-client privilege if the employee had consented to employer monitoring.

[105] *See, e.g.*, William P. Matthews, Comment, *Encoded Confidences: Electronic Mail, the Internet, and the Attorney-Client Privilege*, 45 KAN. L. REV. 273, 287 (1996);

the Internet that include "nearly unrestrained access by system administrators to e-mail accounts and the interception of e-mail transmissions by third parties."[106] Two commentators, Peter Jarvis and Bradley Tellam, have addressed the issue by comparing e-mail communications with traditional modes of attorney-client communications.[107]

Jarvis and Tellam argue that the difficulty in creating confidential communications over the Internet is not the form of the communication, but rather the medium's lack of confidentiality.[108] The commentators assert that "computer communicat[ions] through a 'reputable' commercial e-mail provider" would satisfy the privilege, and this assertion hinges on the greater security that "reputable" providers provide.[109] However, threats from those that can intercept or otherwise violate the computer network are the prime concern, and the serious security risks associated with the Internet pose threats to the confidentiality of a communication.[110] Thus, if there is no reasonable expectation of privacy due to various security risks of the Internet, then the communication is not "confidential." If the communication is not confidential, then the attorney-client privilege will not attach.

2. *E-mailing from a Work Computer as a Waiver of the Attorney-Client Privilege*

Even if an e-mail communication is found to have originated in confidence, there is a further problem that may prevent a successful claim of attorney-client privilege. The attorney-client privilege has the additional requirement that the confidentiality created must be subsequently maintained—that is, there must not be a waiver of the privilege.[111] This requirement is threatened by workplace monitoring of employees' computer behavior. Workplace monitoring may constitute a waiver of the attorney-client privilege if these activities involve the subsequent sharing of the confidential information with a third party.[112]

The client can expressly waive the attorney-client privilege, but the client or attorney may also inadvertently waive the privilege by actions such as revealing the contents of privileged communications to parties without a

---

Peter R. Jarvis & Bradley F. Tellam, *The Internet: New Dangers of Ethics Traps*, 56 OR. ST. B. BULL. 17 (1995).

[106] Matthews, *supra* note 105, at 287.

[107] See Jarvis & Tellam, *supra* note 105, at 7, 17.

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] RICE, *supra* note 25, § 2:1, at 6–10.

[112] Nichols, *supra* note 26, at 10.

need to know.[113] A client waives the attorney-client privilege if he discloses the contents of a privileged communication to anyone who is not an interested party in the action, and this may be true even if the disclosure is inadvertent.[114] In some jurisdictions, a waiver of the attorney-client privilege can result from inadvertence due to the failure by the attorney or the client to take precautions to keep a communication confidential.[115] Thus, if workplace monitoring is construed as disclosing the contents of a privileged communication to the employer, even though this disclosure is likely inadvertent by the employee, it may constitute a waiver of the privilege.[116]

In addition, a client can waive the attorney-client privilege if a third party is privy to the communication. Thus, in the context of communications over the Internet, a court could find a waiver of the privilege if an e-mail communication were accessed by a third party.[117] In this respect, an employer's monitoring of its employees' e-mail use has implications of maintaining confidentiality. If an employer's access to its employees' e-mails means that it is "privy" to the communications, then this constitutes a disclosure of the communication to a third party, and that communication may be deemed "waived" and may be used against the employee in litigation.

Furthermore, it has also been suggested that workplace monitoring is analogous to intentional inclusion to constitute a waiver of the attorney-client privilege. One commentator proposes that if an employee signs a written contract agreeing that his or her employer can monitor her computer use, that employer should be considered an "intentional recipient" of any personal e-mail because the employee agreed to the workplace monitoring.[118] In these situations, some courts have found that when an employee knows his employer is monitoring his e-mail, he cannot have an expectation of privacy

---

[113] United States v. Ryans, 903 F.2d 731, 741 n.13 (10th Cir. 1990) (finding that a client can inadvertently waive privilege if a third party overhears a confidential conversation).

[114] Messer, *supra* note 24, at 92.

[115] *See, e.g.*, Texaco P.R. Inc. v. Dep't. of Consumer Affairs, 60 F.3d 867, 883 (1st Cir. 1995) (finding that the waiver of privilege by inadvertent disclosure of documents also waived the privilege for all other related documents); Alldread v. City of Grenada, 988 F.2d 1425, 1434 (5th Cir. 1993) (finding no error in district court's decision finding attorney-client privilege for inadvertently produced materials); Weil v. Inv./Indicators, Research & Mgmt., Inc., 647 F.2d 18, 24 (9th Cir. 1981) ("'Inadvertence' of disclosure does not as a matter of law prevent the occurrence of the waiver."). *See also* HÉBERT supp., *supra* note 2, § 8A:33:50, at 345 ("The privilege is generally not waived by inadvertence, *unless* the inadvertence suggests that the possessor of the privilege did not take steps to maintain the confidentiality of the communications.") (emphasis added).

[116] *See* Leonard, *supra* note 84, at 867.

[117] Leonard, *supra* note 84, at 869–70.

[118] Messer, *supra* note 23, at 93.

when he accesses confidential e-mail at work.[119] Thus, whether a disclosure is deemed inadvertent or intentional, workplace monitoring has the potential to create waivers of the attorney-client privilege if a client is communicating with his attorney while at work.

IV. THE NEW LINE OF EMPLOYEE PRIVACY CASES: ATTORNEY-CLIENT COMMUNICATIONS

A new issue arising in the area of employee privacy occurs when an employee communicates with his private attorney on an employer-owned computer.[120] Several courts have addressed this issue to determine whether the communication can still be protected by the attorney-client privilege.[121] An employee's expectation of privacy plays a central role in determining if attorney-client privilege exists.[122] Importantly, an employer's policies regarding the workplace and computer use may diminish an employee's expectation of privacy in personal communications sent via e-mail.[123]

To date, courts have not developed a bright line approach for determining when the attorney-client privilege protects communications from an employer-issued computer. Several courts have treated the traditional expectation of privacy cases as controlling, balancing the four factors[124] to determine if the employee had a reasonable expectation of privacy in his e-mails to his attorney.[125] However, one court has held that the expectation of privacy cases are not controlling in the unique context of the attorney-client

---

[119] *Id.* at 94.

[120] *See* HÉBERT, *supra* note 2, § 8A:33:50, at 344–45 ("A number of recent cases have involved contentions by employers that they are entitled to discover the content of electronic communications between present and former employees and the employees' attorneys, on the ground that the attorney-client privilege has been waived with respect to those communications because those communications are accessible to the employer.").

[121] *See, e.g.*, Curto v. Med. World Commc'n, Inc., No. 03CV632, 2006 WL 1318387 (E.D.N.Y. May 15, 2006); Kaufman v. SunGard Inv. Sys., No. 05-cv-1236(JLL), 2006 WL 1307882 (D.N.J. May 10, 2006); *In re* Asia Global Crossing, Ltd., 322 B.R. 247 (Bankr. S.D.N.Y. 2005); Nat'l Econ. Research Assoc., Inc. v. Evans, No. 04-2618-BLS2, 2006 WL 2440008 (Mass. Super. Ct. Aug. 3, 2006). These four cases deal with both the situation of whether the communication was originally made in confidence (*see infra*, Part III.C.1) and whether the attorney-client privilege was subsequently waived (*see infra*, Part III.C.2).

[122] TBG Ins. Servs. Corp. v. Superior Court of L.A. County, 96 Cal. App. 4th 433, 449 (Cal. Ct. App. 2002).

[123] Nichols, *supra* note 26.

[124] *See supra* Part II for a discussion of the four factors traditionally balanced by courts.

[125] *See Nat'l Econ.*, 2006 WL 2440008; *Asia Global*, 322 B.R. 247; *Kaufman*, 2006 WL 1307882.

privilege and has developed its own approach to handling these types of employee privacy cases.[126]

A. *Cases Following the Traditional Expectation of Privacy Cases*

1. *Communications Made in Confidence*

For the attorney-client privilege to attach to a communication, "a communication must be made in confidence of the relationship and under circumstances from which it may reasonably be presumed that it will remain in confidence."[127] Recently, the Superior Court of Massachusetts determined whether the attorney-client privilege attached to a communication made by an employee to his attorney on a work-provided laptop.[128] In *National Economic Research Associates, Inc. v. Evans*, National Economic Research Associates, Inc. (NERA) moved to compel its former employee Evans to disclose attorney-client communications between Evans and his private attorney.[129] The attorney-client communications were conducted by e-mail over a laptop provided by NERA, but Evans had sent and received e-mails from his personal, password-protected e-mail account with Yahoo rather than his NERA e-mail address.[130] Each of the attorney-client communications that were sent or retrieved by Evans with the NERA-issued laptop were stored in the hard drive of the laptop, and they could be retrieved by a person with substantial computer expertise.[131] When Evans resigned from NERA, NERA retained a computer forensic expert to search the hard disk of Evans' NERA-issued laptop.[132] During the forensic search, the expert was able to retrieve

---

[126] *Curto*, 2006 WL 1318387, at *5.

[127] Wilcoxon v. United States, 231 F.2d 384, 386 (10th Cir. 1956), *cert. denied*, 351 U.S. 943 (1956).

[128] *Nat'l Econ.*, 2006 WL 2440008, at *1.

[129] *Id.* at *1. Before leaving NERA to join his new employer, LECG, Evans conferred with his private attorney regarding various legal matters concerning his departure from NERA and the commencement of his employment at LECG. *Id.*

[130] *Id.* Evans often used the laptop issued to him by NERA to send and retrieve these e-mails via the Internet.

[131] Unknown to Evans, when one accesses information through the Internet from a private e-mail account, such as an account with Yahoo, "all the information that is accessed is copied via a 'screen shot' onto a temporary Internet file on that computer's hard drive." *Id.* at *1.

[132] *Id.* at *2.

from the hard disk various attorney-client communications between Evans and his private attorney.[133]

In its motion to compel, NERA argued that the attorney-client privilege never attached to the communications.[134] Evans' use of his NERA laptop was governed by the policies set forth in NERA's Policies and Procedures Manual ("Manual"), which was posted on NERA's Intranet.[135] NERA contended that the warnings in the Manual provided reasonable notice to Evans that the hard disk of his laptop belonged to NERA and could be read by NERA.[136] As a result, NERA argued that the e-mailed attorney-client communications "should not be found to have been made 'in confidence' because Evans reasonably should have understood that they could be read by NERA."[137]

The court, however, held that the attorney-client communications were in fact protected by the attorney-client privilege.[138] To determine confidentiality, the court examined the reasonable expectation of privacy that Evans had in the communications.[139] The court found that the Manual did

---

[133] *Nat'l Econ.*, 2006 WL 2440008, at *2 (stating that all of the material discovered derived from Evans' Yahoo e-mail account, and none were made on NERA's Intranet or stored in any document that could be retrieved by Window's Explorer).

[134] *Id.* at *3 (arguing that because Evans should have recognized that the hard disk on the laptop belonged to NERA and was subject to review by NERA, Evans cannot meet his burden of establishing that "the communications were made in confidence").

[135] *Id.* The Manual stated:

> The personal use of e-mail, the Internet and telephones should be kept to a minimum for both productivity and financial reasons. All computer resources are the property of the Company. To the extent permitted by law and any applicable agreements, the Company may, from time to time and at its discretion, review any information sent or stored using these resources. Be aware that e-mails are not confidential and the Company may read them during routine checks.

Id. at *2. The Manual also stated, "NERA does permit the use of Internet resources . . . for personal use provided such use results in personal time savings that can be (at least partially) applied toward work . . . ." *Id.* at *3.

[136] *Id.* at *3.

[137] *Nat'l Econ.*, 2006 WL 2440008, at *3.

[138] *Id.* at *4 (finding that Evans had met the burden of "establishing that a privilege exists . . . if adequate steps have been taken to ensure a document's confidentiality") (citing Matter of Reorganization of Elec. Mut. Liab. Ins. Co. (Bermuda), 681 N.E. 2d 838, 841 (1997)).

[139] *Id.* Discussing Evans' reasonable expectation of privacy, the court noted that an attorney-client privilege is not confidential and therefore not protected by the attorney-client privilege if "the communication was made in the presence of a third party who was not a necessary agent of the attorney or the client." *Id.* at *3. *See also* Commonwealth v. Rosenberg, 573 N.E.2d 949, 954 n.10 (1991) (attorney-client communication not

not expressly declare that it would monitor the *content* of Internet communications. Rather, "it simply declared that NERA would monitor the Internet *sites* visited."[140] More importantly, the court emphasized, the Manual did not expressly declare, or even implicitly suggest, that NERA would monitor the content of e-mail communications made from an employee's personal e-mail account via the Internet whenever those communications were viewed on a NERA-issued computer.[141] Therefore, Evans had a reasonable expectation of privacy in the communications because the Manual did not warn employees that the employer would monitor e-mails from a personal account if they were viewed on an employer-issued computer.[142]

Furthermore, the court rejected NERA's contention that any reasonable person "would have known that the hard disk of a computer makes a 'screen shot' of all it sees, which the computer then stores in a temporary file, including e-mails retrieved from a private password-protected e-mail account on the Internet."[143] The court concluded that since a reasonable person in Evans' position would not have recognized that e-mail communications with his private attorney made from a private Internet e-mail account could be read by NERA simply by examining the hard disk of its laptop, Evans could not reasonably have understood that these attorney-client communications could be "overheard" by NERA.[144]

Thus, the *National Economic* court relied on the factors traditionally employed in the privacy cases to determine whether the defendant had a reasonable expectation of privacy in the communications. Finding that Evans did have a reasonable expectation of privacy because the employer's manual did not explicitly declare that it would monitor the content of e-mails sent or received, the court found the attorney-client communications were protected by the attorney-client privilege.[145]

---

privileged if the communication was made privately but it was understood that the information communicated was to be conveyed to others).

[140] *Nat'l Econ.*, 2006 WL 2440008, at *3.

[141] *Id.* Nor did NERA warn its employees that the content of such e-mail communications was stored on the hard disk of a NERA-issued computer and therefore capable of being read by NERA. *Id.*

[142] *Id.*

[143] *Id.* at *4 ("This Court does not agree that any reasonable person would have known this information. Certainly, until this motion, this Court did not know of the routine storing of 'screen shots' from private Internet e-mail accounts on a computer's hard disk.").

[144] *Id.* at *5.

[145] *See Nat'l Econ.*, 2006 WL 2440008, at *2–5.

2. *Waiver of Privilege*

When the attorney-client privilege is present, the client is the exclusive holder of the privilege, and the communication will remain privileged, as long as the client does nothing to waive the privilege.[146] Generally, if the client discusses or otherwise reveals the communication to a third party, the communication is no longer protected by the attorney-client privilege.[147] Recently, there have been several cases that have examined the waiver of attorney-client privilege in the context of an employee's communications over a work-issued computer.

In *In re Asia Global Crossing, Ltd.*, the issue was "whether an employee's use of the company e-mail system to communicate with his personal attorney destroys the attorney-client . . . [privilege] in the e-mails . . . ."[148] The court began with an analysis of the confidentiality of e-mail communication in general, noting that "[a]lthough e-mail communication, like any other form of communication, carries the risk of unauthorized disclosure, the prevailing view is that lawyers and clients may communicate confidential information through unencrypted e-mail with a reasonable expectation of confidentiality and privacy."[149] The court noted that, consistent with this trend, New York and California have enacted laws that provide some protection to e-mail communication.[150] Accordingly, the

---

[146] *See* CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, EVIDENCE § 5.6, at 352 (1995).

[147] *See* Wilcoxon v. United States, 231 F.2d 384, 386 (10th Cir. 1956).

[148] *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 251 (Bankr. S.D.N.Y. 2005). In this case, the trustee in bankruptcy moved to compel the production of the e-mail communications between former officers and employees of the debtor and their private attorneys in connection with an investigation of those officers, contending that the use of the employer e-mail system waived any attorney-client privilege that may have otherwise existed. *Id.* at 252–55. The case also concerned waiver of the work product and joint defense privileges in the e-mails; however, these topics are beyond the scope of this Note.

[149] *Id.* at 256 (citing, e.g., N.Y.C. Ass'n. Bar Comm. Prof'l Judicial Ethics, Formal Op. 2000-1, 2000 WL 704689 (2000); ABA Comm. on Ethics and Prof'l Responsibility Formal Op. 99-413 (1999), *available at* http://www.abanet.org/cpr/fo99-413.html; N.Y. State Bar Ass'n. Comm. on Prof'l Ethics, Eth. Op. 709, 1998 WL 957924 (1998). *See generally* Audrey Jordan, Note, *Does Unencrypted E-Mail Protect Client Confidentiality?*, 27 AM. J. TRIAL ADVOC. 623, 626 n.25 (2004) (referencing ethical opinions from twenty-three State bar associations).

[150] *Asia Global*, 322 B.R. at 255. N.Y. C.P.L.R. § 4548 (McKinney 1999) states that a privileged communication does not lose its privileged character for the sole reason that it was sent by e-mail or because persons necessary for the delivery or facilitation of the e-mail may have access to its content. *Accord* CAL EVID. CODE § 917(b) (West 2004).

court concluded that "the transmission of a privileged communication through unencrypted e-mail does not, without more, destroy the privilege."[151]

Due to the novelty of the issue, the *Asia Global* court was unable to locate any decisions discussing the confidentiality of an employee's e-mails in the context of the attorney-client privilege.[152] However, the court looked to case law pertaining to an "employee's expectation of privacy in his office computer and the company e-mail system" for guidance.[153] The court began by stating that "as with attorney-client confidentiality, the expectation of privacy has objective and subjective components."[154] To determine whether the employee has a reasonable expectation of privacy, the court used the same considerations traditionally used to assess reasonable expectations of privacy and relied on four factors:

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?[155]

Applying the four factors, the question of privilege comes down to "whether the intent to communicate in confidence was objectively

---

[151] *Asia Global*, 322 B.R. at 256.

[152] *Id.*

[153] *Id.* ("The Court's own research has not located any decisions that discuss the confidentiality of the employee's e-mails in terms of the attorney-client privilege. Several courts have, however, addressed the analogous question of the employee's expectation of privacy in his office computer and the company e-mail system. These cases offer guidance . . . .").

[154] *Id.* at 257 ("For Fourth Amendment purposes, the person asserting the right must demonstrate that he has 'a subjective expectation of privacy . . . that society accepts as objectively reasonable.'") (citing California v. Greenwood, 486 U.S. 35, 39 (1988)). The court further explained, "Similarly, one claiming an 'intrusion on seclusion' [under common law principles] must show . . . a subjective expectation of privacy and that the expectation is objectively reasonable." *Asia Global*, 322 B.R. at 257.

[155] *Asia Global*, 322 B.R. at 257. *See also* United States v. Slanina v. 283 F.3d 670, 676–77 (5th Cir. 2002); Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002); Leventhal v. Knapeck, 266 F.3d 64, 74 (2d. Cir. 2001); United States v. Simons, 206 F.3d 392, 398 & n.8 (4th Cir. 2000); Thygeson v. U.S. Bancorp, No. CV-03-467, 2004 WL 2066746, at *20 (D. Or. Sept., 15, 2004); Haynes v. Office of the Attorney General, 298 F. Supp. 2d, 1154, 1161–62 (D. Kan. 2003); Kelleher v. City of Reading, No. Civ. A. 01-3386, 2002 WL 1067442, at *8 (E.D. Pa. May 29, 2002); Garrity v. John Hancock Mutual Life Ins. Co., No. Civ. A. 00-12143, 2002 WL 974676, at *1–2 (D. Mass. May 7, 2002). *See also infra* Part II discussion for cases cited by the *Asia Global* court that consider these four factors to determine reasonable expectations of privacy.

reasonable."[156] The court noted that "[t]here is a close correlation between the objectively reasonable expectation of privacy and the objective reasonableness of the intent that a communication between a lawyer and a client was given in confidence."[157] Accordingly, the court concluded that "the objective reasonableness of that intent will depend on the company's e-mail policies regarding use and monitoring, its access to the e-mail system, and the notice provided to the employees."[158] Thus, the *Asia Global* court followed the traditional employee privacy law analysis in the context of attorney-client communications and determined that the privilege is not waived where the intent to communicate in confidence was objectively reasonable.[159]

The U.S. District Court for the District of New Jersey similarly followed the traditional privacy law cases in a case concerning an employee communicating with her personal attorney over a work-provided computer.[160] In *Kaufman v. SunGard Investment System*, Kaufman and OSI, a financial company owned by Kaufman, initiated suit against SunGard alleging, among other claims, breach of contract.[161] SunGard then filed an answer and counterclaim, asserting state law claims against Kaufman based on the alleged disclosure of SunGard confidential information.[162] Among the files that SunGard sought to obtain were deleted files that had been recovered, which consisted of e-mails between Kaufman and her private attorneys.[163] These e-mails were "sent from and received on SunGard's e-

---

[156] *Asia Global*, 322 B.R. at 258.

[157] *Id.* at 258–59.

[158] *Id.* at 259 (indicating that if the company had a policy of monitoring e-mail that was communicated to the officers, the use of the e-mail system was "like placing a copy of that message in the company files" because anyone with lawful access to the system could potentially review those e-mails). Ultimately, however, the evidence was equivocal regarding the existence or notice of company policies banning certain uses or monitoring employee e-mails. *Id.* Therefore, the court was unable to determine as a matter of law whether the employees' use of the company e-mail system to communicate with their attorneys eliminated any existing attorney-client privilege. *Id.* at 261.

[159] *See Asia Global*, 322 B.R. at 256–61.

[160] Kaufman v. SunGard Inv. Sys., No. 05-cv-1236 (JLL), 2006 WL 1307882 (D.N.J. May 10, 2006).

[161] *Id.* at *1. The breach of contract was in connection with SunGard's acquisition of OSI's assets and hiring of Kaufman as senior executive. *Id.*

[162] *Id.*

[163] *Id.* The court categorized the relevant exchanged e-mails into two categories. The first category was e-mail communications exchanged prior to the closing date (SunGard's purchase of OSI's assets), which remained on OSI computers after closing because OSI continued to operate at the same location. The second category was e-mails between Kaufman and her attorneys after the closing date. *Id.*

mail system during Kaufman's employment with SunGard."[164] In her opposition to the order to show cause, Kaufman asserted that the restored e-mails were protected by her attorney-client privilege and therefore were not discoverable.[165] In opposition, however, SunGard argued that Kaufman had waived the attorney-client privilege to her confidential communications.[166]

The magistrate judge had earlier ruled that all of the communications were discoverable because Kaufman waived the attorney-client privilege, and the district court agreed.[167] With respect to the post-closing attorney-client communications,[168] the court focused on the reasonable expectation of privacy analysis that underlies traditional employee privacy in the workplace.[169] The District Court upheld the magistrate judge's ruling that "any privilege attached to the [p]ost-[c]losing [c]ommunications was waived because Kaufman knowingly utilized SunGard's network with the knowledge that company policy provided that SunGard could search and monitor email communications at any time."[170] The court's reasoning rested on an expectation of privacy analysis. The court found that Kaufman agreed to abide by SunGard company property policy[171] and that all information and e-mails stored on SunGard's computer systems was SunGard property. In addition, SunGard's policy also provided that all e-mails were subject to

---

[164] *Kaufman*, 2006 WL 1307882, at *1. The e-mails had been sent and received on laptop computers issued to the plaintiff by the employer during her employment. When she returned the laptops to the employer, she attempted to delete the messages, but they were recovered by a computer technician. *Id.*

[165] *Id.*

[166] *Id.* (arguing that Kaufman waived the attorney-client privilege as to the pre-closing communications by failing to delete them from the computer and that the attorney-client privilege with respect to the post-closing communications had been waived based on SunGard's employment policies governing e-mail communications).

[167] *Id.* at *2.

[168] The court initially analyzed the pre-closing communications, applying the rule that a voluntary disclosure of a privileged communication waives the privilege. *Id.* The court found that Kaufman "intended to transfer the information by failing to take reasonable measures to withhold the emails or ensure the confidentiality of the emails at issue." *Kaufman*, 2006 WL 1307882, at *3. Accordingly, the court found that Kaufman's actions were deliberate so as to waive the privilege attached to the documents. *Id.* To support this conclusion, the court noted that "the express language of the Acquisition Agreement as well as the conduct of the parties lead [the magistrate judge] to conclude that the parties intended for the e-mail communications which took place prior to closing to be transferred along with other information." *Id.*

[169] *See id.* at *4. *See also infra* Part II discussing these cases.

[170] *Kaufman*, 2006 WL 1307882, at *4.

[171] *Id.* (noting that "SunGard's 'Use of Company Property and Services' provided that 'Company Property' included, for instance, 'information stored on computers' and 'e-mail'").

monitoring.[172] Based on Kaufman's agreement to abide by SunGard's company policy, the court held that Kaufman had no reasonable expectation of privacy as to his private communications with his attorney.[173]

The recent cases *National Economic*, *Asia Global*, and *Kaufman* illustrate the approach three courts have taken on the issue of an employee communicating with his private attorney when the employer may have access to that communication. By following the traditional privacy law cases,[174] these courts focused on whether the employer had a monitoring policy and whether the employee was aware of such a policy to determine whether the employee had a reasonable expectation of privacy in the e-mail communications.[175]

B. *The Expectation of Privacy Cases May Not Be Controlling*

Despite several courts analyzing the attorney-client privilege issue by following the traditional expectation of privacy cases, one recent case concerning the attorney-client privilege of an employee has not followed that trend.[176] In *Curto v. Medical World Communications, Inc.*, Plaintiff Curto was employed by Medical World Communications ("MWC") from August 1995 to October 2003.[177] In 1999, Curto signed an acknowledgement of her receipt and understanding of MWC's "E-mail/Computer Privacy Policy," contained within the Employee Handbook, which governed the use of its computer resources.[178] Beginning in May 2002, Curto worked primarily out

---

[172] *Id.* The court found that SunGard warned its employees that SunGard "has the right to access and inspect all electronic systems and physical property belonging to it. Employees should not expect that any items created with, stored on, or stored within Company property will remain private. This includes . . . computer files and electronic mail, even if protected with a password." *Id.* SunGard further notified all employees that SunGard "reserves the right to monitor and inspect network or Internet usage and e-mail" and that "any e-mail may be subject to monitoring, search or interception at any time, with or without notice to the sender or recipient." *Id.*

[173] *Id.* at *4. The court noted at the end of its opinion that the Plaintiff filed a motion for reconsideration that was denied. The court therefore did not address Kaufman's explanation that personal communications with her attorneys were exchanged at the office out of necessity arising from the long business hours at SunGard. *Kaufman*, 2006 WL 1307882, at *4.

[174] *See supra* Part I.

[175] *See Kaufman*, 2006 WL 1307882, at *4; Nat'l Econ. Research Assocs., Inc. v. Evans, No. 04-2618-BLS2, 2006 WL 2440008, at *4 (Mass. Super. Aug. 3, 2006); *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 251 (Bankr. S.D.N.Y. 2005).

[176] Curto v. Med. World Commc'ns, Inc., No. 03CV6327, 2006 WL 1318387 (E.D.N.Y. May 15, 2006).

[177] *Id.*

[178] *Id.* at *1. The policy provided in part:

of her home office and was assigned employer-provided laptop computers.[179] Before transferring from a Macintosh laptop ("Mac") to a Dell laptop ("Dell"), Curto deleted her personal files from the Mac, including notes and e-mails she had sent her personal attorneys regarding the present action.[180] The Mac laptop was then returned to MWC.[181] Curto then used the Dell laptop in her home office until she was terminated in 2003, at which time she returned the Dell to MWC.[182]

Almost two years later, MWC was able to restore portions of the computer files and e-mails that had been deleted by Curto.[183] MWC sought to use the documents in the present action, but Curto's counsel asserted that many of these documents were protected from disclosure by the attorney-client privilege.[184] The court thus had to determine whether Curto was entitled to assert the attorney-client privilege to require the documents to be returned and not disclosed by defendants.[185]

In line with several other courts following the expectation of privacy cases, the defendants argued that "numerous federal courts have held that an employee has no expectation in workplace computer files where . . . company guidelines and policy explicitly inform the employee that no expectation of privacy exists."[186] However, in contrast with the courts in *National Economic*, *Asia Global*, and *Kaufman*, the *Curto* court did not

---

> Employees should not have an expectation of privacy in anything they create, store, send, or receive on the computer system . . . . Employees expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network. Employees consent to allowing personnel of [MWC] to access and review all materials employees create, store, send, or receive on the computer or through the Internet or any computer network.

Id.

[179] *Id.* Curto was assigned a Company-owned Macintosh laptop computer ("Mac") until May 2003, when she was told she would be converting to a Dell laptop computer ("Dell"). As a result, Curto had her files from the Mac transferred to the new Dell.

[180] *Id.*

[181] *Id.*

[182] *Curto*, 2006 WL 1318387, at *1. Before she returned the Dell, she again deleted all personal files and written communications to private counsel. *Id.*

[183] *Id.* MWC hired a forensic consultant to inspect the Mac and Dell laptop computers assigned to Curto; the consultant was able to recover portions of the computer files and e-mails.

[184] *Id.* at *1.

[185] *See id.* at *2.

[186] *Id.* at *5 (citing Muick v. Glenayre, 280 F.3d 741, 743 (7th Cir. 2002); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000); Thygeson v. Bancorp, No. CV-03-467–ST, 2004 WL 2066746 (D. Or. Sept. 15, 2004) at *18–21; Kelleher v. City of Reading, No. CIV.A.01-3386, 2002 WL 1067442 at *7–8 (E.D. Pa. May 29, 2002)).

believe that the expectation of privacy cases were controlling.[187] The court reasoned that

> "[a]ll of [the expectation of privacy cases cited by defendants], however, arise in the context of an employee asserting a right to privacy claim, either under the Fourth Amendment or common law. While these cases may be analogous, they are not controlling as they do not address the confidentiality of employee's e-mails and personal computer files with regard to the attorney-client privilege . . . ."[188]

Thus, the *Curto* court found that the traditional expectation of privacy cases were *not* controlling in the context of the attorney-client privilege.

The court further explained that not only do the attorney-client privilege cases arise in a different context, the *Curto* case was also factually distinguishable from the traditional expectation of privacy cases in an important way—none of the expectation of privacy cases involved an employee working from a *home* office.[189] Thus, after reviewing the right to

---

[187] *Curto*, 2006 WL 1318387, at *5 (declaring that "[t]he [e]xpectation of [p]rivacy [c]ases are not [c]ontrolling").

[188] *Id.* The court saw it as important to distinguish the different context of cases dealing with Fourth Amendment or common law privacy claims versus privacy claims dealing with the attorney-client privilege. *Id.* For example, it noted that the Second Circuit had the opportunity to rule on an expectation of privacy case under the Fourth Amendment in Leventhal v. Knapek. *Id.* In *Leventhal*, the Second Circuit stated that in determining whether a public employee has a reasonable expectation of privacy in his office computer, "the context of the employment relation" should be considered. 266 F.3d 64, 73 (2d Cir. 2001) (quoting O'Connor v. Ortega, 480 U.S. 709, 717 (1987). The court then found that the plaintiff-employee had a reasonable expectation of privacy in the contents of his office computer as the employer had neither a general practice of monitoring nor a policy governing computer usage. *Id.* The *Curto* court emphasized that the *Leventhal* case is distinguishable because it "involves an employee's right to privacy under the Fourth Amendment and *does not involve the interplay of this right with the attorney-client privilege* . . . ." *Curto*, 2006 WL 1318387 at *6 (emphasis added).

[189] *Curto*, 2006 WL 1318387, at *5. The court noted that this distinction is particularly significant in Thygeson v. U.S. Bancorp, CV-03-467-ST, 2004 WL 2066746 (D. Or. Sept. 15, 2004). In *Thygeson*, the court found that the plaintiff-employee had "no reasonable expectation of privacy" in files he stored in his personal folder on his computer and in his personal e-mail account because his employer had an "explicit policy banning personal use of office computers and permitting monitoring," and because the employer retrieved such information by accessing its own computer network. *Thygeson*, 2004 WL 2066746, at *21. The court found the employer "retained the key" to plaintiff's files as it "was able to remotely search [plaintiff's] personal files on the network." *Id.* at *19. However, in the *Curto* case, Curto's laptops were not connected to MWC's computer server and were not located in MWC's offices. *Curto*, 2006 WL 1318387, at *5. Therefore, "MWC was not able to monitor [Curto's] activity on her home-based laptops or intercept her e-mails at any time." *Id.* When Curto did have to return her

privacy cases cited by the defendants, the court did not believe such cases were controlling. The court emphasized the Supreme Court's instruction in *O'Connor*: "Given the great variety of work environments . . . the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis."[190] In light of these observations, the *Curto* court was unwilling to treat the expectation of privacy cases as controlling in the issue of employee privacy with respect to privileged attorney-client communications.

V. A NEW WAY TO LOOK AT THE ATTORNEY-CLIENT PRIVILEGE IN EMPLOYEE PRIVACY CASES

If the expectation of privacy cases are not controlling (i.e., if the *Curto* approach is followed), courts are free to develop their own way to analyze cases in which an employee communicates with his private attorney on an employer-owned computer and the employer has access to the communication. There are several factors to consider to strike an appropriate balance between protecting employees' rights to privacy and yet allowing employers to monitor their employees' business activities. Ultimately, however, courts, legislatures, and ABA officials should strive to protect employee privacy and the attorney-client privilege. This Part discusses possible approaches to protecting the privilege through solutions such as following the *Curto* court's approach; through legislative enactments such as an amendment to the ECPA or state legislation; and, finally, through an American Bar Association requirement of precaution.

---

laptops, she deleted all personal files. *Id.* at *1. Thus, according to the *Curto* court, it was reasonable for Curto to believe that the e-mails she sent and the personal documents she stored on her laptops were confidential. *Id.* at *5.

The *Curto* court also distinguished *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000), factually. *See Curto*, 2006 WL 1318387, at *6. In *Simons*, the company's monitoring policy stated that electronic auditing "shall be implemented" and that "[u]sers shall . . . [u]nderstand [the employer] will periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate." *Simons*, 206 F.3d at 395–96. The Fourth Circuit concluded that such language "placed employees on notice that they could not reasonably expect that their Internet activity would be private." *Id.* at 398. In *Curto* in contrast, the employer's policy declared: "Employees understand that [MWC] *may* use human or automated means to monitor use of computer resources." *Curto*, 2006 WL 1318387, at *6. The court found that "[n]ot only is the wording in the policy at issue ambiguous as to whether MWC will conduct audits, because [Curto] worked at home . . . any such monitoring would have had to have been preceded by notice to [Curto]." *Id.*

[190] *Curto*, 2006 WL 1318387 at *6 (citing O'Connor v. Ortega, 480 U.S. 709, 718 (1987)). The court further noted that "[a]lthough the instant case involves the juxtaposition of the right to privacy with the attorney-client privilege . . . this instruction is relevant nonetheless." *Curto*, 2006 WL 1318387, at *6.

A. *The Attorney-Client Privilege Should Be Protected*

There are several reasons given by employers justifying their need to electronically monitor their employees.[191] It is clear that there are legitimate reasons for employers to monitor their employees' computer activity, and, as one author has noted, it seems "very unlikely that employees will be able to challenge successfully . . . employer use of computer monitoring of employees, *at least to the extent that what is being monitored is some aspect of the way that employees perform their jobs*."[192] However, to the extent that the computer monitoring reveals non-work-related information about an employee, the monitoring no longer seems justified by the employers' legitimate business justifications.[193] Thus, employers are not necessarily justified in monitoring non-work-related computer usage, and the privacy of employees with respect to non-work-related matters, such as their personal communications with their private attorneys, should be protected.

Moreover, the attorney-client privilege demands protection because it is extremely important in today's legal landscape. The attorney-client privilege "may well be the pivotal element of the modern American lawyer's professional functions."[194] "The attorney-client privilege ensures candid, independent, and honest assessments from attorneys by protecting information exchanges between the attorney and client for the purpose of securing legal advice."[195] While suppressing certain information shared between the attorney and client "may prevent the fact-finder from ascertaining a full and accurate account of the truth," the recognition of the attorney-client privilege reflects a "societal judgment that this harm is outweighed by the importance of a client having confidential consultation

---

[191] *See supra* Part II. For a detailed discussion of employer justifications for use of electronic monitoring and surveillance, see HÉBERT, *supra* note 2, § 8A:2, at 17–23.

[192] HÉBERT, *supra* note 2, § 8A:7, at 52 (emphasis added).

[193] *Id.* at 53.

[194] Geoffrey C. Hazard, Jr., *An Historical Perspective on the Attorney-Client Privilege*, 66 CAL. L. REV. 1061, 1061 (1978) (discussing the importance of the attorney-client privilege and claiming that the privilege "is considered indispensable to the lawyer's function as advocate on the theory that the advocate can adequately prepare a case only if the client is free to disclose everything, bad as well as good"). "The privilege is also considered necessary to the lawyer's function as confidential counselor in law on the similar theory that the legal counselor can properly advise the client what to do only if the client is free to make full disclosure." *Id.*

[195] Lisa Plush, *A Balanced Approach to Government Attorney-Client Privilege in the Confirmation Setting*, 19 GEO. J. LEGAL ETHICS 907, 910 (2006).

with his lawyer."[196] Thus, because the attorney-client privilege is "required for the attorney to function most effectively," it is imperative that this privilege be protected.[197]

The attorney-client privilege also faces new threats as employees are increasingly working outside of the office and working longer hours; as a result of these new dangers, adequate protection of the privilege is required. More and more, companies are employing "remote workers," which are employees who work from home, using a work-provided computer.[198] Remote workers have been commonplace in businesses for several years,[199] and the number of remote workers is continually on the rise.[200] As the number of people working from home increases, the number of employees using their work-related computers for personal use is also on the rise.[201] The personal use of work computers by remote workers has the potential to increase the problems of keeping attorney-client confidences privileged.[202]

---

[196] *Id.* (reporting that courts acknowledge privileges because their purpose outweighs the merit of the evidence that would be introduced without the claim of privilege).

[197] *Id.* at 911.

[198] *See* Hickey, *supra* note 24.

[199] *See id.*

[200] Andrew R. Hickey, *Mobile, Remote Workers Putting Strain on IT*, SEARCHNETWORKING.COM, Dec. 12, 2005, http://searchmobilecomputing.techtarget.com/news/article/0,289142,sid40_gci1151501,00.html. One study predicts that remote workers in the U.S. alone will reach 103 million by 2008. *Id.* This is a spike in numbers, as the U.S. Bureau of Labor Statistics estimated that there were twenty-five million employees working from home at least once a month in 2001. Paula Jacobs, *On the Road Again: Keeping Remote Workers Connected*, SearchExchange.com, Aug. 30, 2004, http://searchexchange.techtarget.com/news/article/0,289142,sid43_gci1003074,00.html.

[201] Hickey, *supra* note 24 (reporting that 30% of remote workers surveyed in the Cisco study claimed to use their computers for personal matters, while 46% said they buy personal items using work computers).

[202] This scenario mirrors the facts of the *Curto* case, as the plaintiff in that case was working from home and the e-mail communications with her private attorney occurred while she was working remotely on an employer-provided computer.

In addition, in *National Economic*, the court refused to find that an employee had waived the attorney-client privilege based on similar concerns about the increasing popularity of remote workers. *See* Nat'l Econ. Research Assoc., Inc. v. Evans, No. 04-2618-BLS2, 2006 WL 2440008, *5 (Mass. Super. Ct. Aug. 3, 2006). In its conclusion, the court explained that "a different result would make it very difficult for employees who travel on business to engage in privileged communications with their attorneys because they could not use the employer-provided laptop nor any hotel computer, because the hotel could access the communication stored on its computer. Instead, the court said, the employee would have to travel with two laptops—the employer's and his or her own." HÉBERT *supra* note 2, at § 8A:33:50, 381 (discussing the reasoning behind the decision of the *National Economic* court).

Moreover, there is also the emerging issue of personal communications being exchanged at work due to the necessity of long working hours.[203] Given the expanding forums in which private e-mails may be exchanged on work computers, it is increasingly important to find ways to protect employees' confidential communications with their private attorneys.

B. *Solutions to the Problem: Possible Ways to Protect Employees' Private Communications with Their Attorneys*

1. *Follow the* Curto *Court's Approach*

The *Curto* court distinguished the situation of an attorney-client communication from the expectation of privacy cases under the Fourth Amendment and common law and determined that the expectation of privacy cases are not controlling in this different context.[204] Embarking on a new approach, the court noted that it has consistently adopted a middle-of-the-road approach in determining whether inadvertent disclosure results in a waiver.[205] In this regard, courts have routinely examined four factors in analyzing whether "the producing party's conduct was so careless as to suggest that it was not concerned with the [protection] of the asserted

---

[203] *See* Kaufman v. SunGard Invest. Sys., No. 05-cv-1236(JLL), 2006 WL 1307882, at *4 (D.N.J. May 10, 2006) (discussing that in a new certificate filed the plaintiff explained that personal communications with her attorneys were exchanged at the office out of necessity arising from the long business hours at SunGard). Even though the court did not address this issue, it demonstrates that long working hours can contribute to increased personal communications by employees on employer-provided computers.

[204] *See* Curto v. Medical World Communications, Inc., No. 03CV6327, 2006 WL 1318387, at *5 (E.D.N.Y. May 15, 2006); *see also supra* Part III.C.

[205] *Curto*, 2006 WL 1318387, at *4. Courts have taken three different approaches to inadvertent disclosure of documents during discovery: (1) the "lenient approach," whereby inadvertent disclosure does not waive the privilege, even with regard to the disclosed documents; (2) the "strict test," wherein inadvertent disclosure waives the privilege regardless of the care taken to prevent the disclosure; or (3) the "middle-of-the-road approach," in which inadvertent disclosure *may* waive the privilege, depending on the circumstances, especially the care taken to prevent disclosure of privileged matter and the existence of prompt efforts to retrieve the document. *See, e.g.*, Kenneth S. Broun & Daniel J. Capra, *Getting Control of Waiver of Privilege in the Federal Courts: A Proposal for a Federal Rule of Evidence* 502, 58 S.C. L. REV. 211, 220 (2006); Michael D. Fielding & Jack Seward, *You Need to Know This: Bankruptcy and Attorney-Client Privilege in the Electronic Age*, 25-JAN AM. BANKR. INST. J. 1, *64 (2007). Akin to the court in *Curto*, the "middle-of-the-road" approach is the approach taken by many recent decisions. *See* Geoff Howard & Andrew Tran, *Electronic Discovery Cost Containment Under the New Federal Rules and Beyond*, 747 PRACTISING L. INST., LITIG. 371, 391 (2006).

privilege."[206] The four relevant factors that courts have been called upon to balance are:

> [1] the reasonableness of the precautions taken by the producing party to prevent inadvertent disclosure of privileged documents; [2] the volume of discovery versus the extent of the specific disclosure [at] issue; [3] the length of time taken by the producing party to rectify the disclosure; and [4] the overarching issue of fairness.[207]

In addition to these traditional four factors, however, the *Curto* court added a fifth factor to the analysis: "whether or not there was enforcement of [any computer usage] policy."[208] The defendant argued that the lower court had erred in adopting this factor. The defendant's argument was that the fifth factor, i.e., "whether or not [defendant] *enforced* its computer usage policy," had not been adopted or followed by any other court, and that this newly imposed requirement was "contrary to well-settled law."[209] The court, however, rejected the defendant's argument and upheld the use of this additional factor.[210]

Because the court was of the view that the right to privacy cases do not control when factual circumstances involve the interplay of privacy rights with the attorney-client privilege, it did not view that the existing cases compelled the conclusion that enforcement may not be a relevant factor.[211] Applying the five factors, the court found that the defendant's lack of

---

[206] *Curto*, 2006 WL 1318387, at *4 (quoting SEC v. Cassano, 189 F.R.D. 83, 85 (S.D.N.Y.1999)).

[207] *Curto*, 2006 WL 1318387, at *2. *See also* Gray v. Bicknell, 86 F.3d 1472, 1484 (8th Cir. 1996); Abbott v. Coyle, No. CV 05-5051(ADS)(WDW), 2006 WL 3780550 (E.D.N.Y. Dec. 21, 2006); Williams v. Sprint/United Management Co., No. 03-2200-JWL-DJW, 2006 WL 1867478 at *9 (D. Kan. July 1, 2006); United States v. Rigas, 281 F. Supp.2d 733, 738 (S.D.N.Y. 2003).

[208] *Curto*, 2006 WL 1318387, at *3. The court, in several instances, also categorized this factor as a "subset" of the first factor, i.e., the reasonableness of the precautions taken by the plaintiff to prevent inadvertent disclosure. *Id.* at *5.

[209] *Id.* at *4.

[210] *Id.* at *4–5.

[211] *Id.* at *6 (heeding to "the Supreme Court's instruction in *O'Connor*: '[g]iven the great variety of work environments, ... the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis'"). To support this conclusion, the court noted that in the *Asia Global* case, "[a]lthough the court ... did not explicitly discuss whether the employer actually monitored employees' computer usage ... it did recognize enforcement as a factor to be considered." *Id.* at *8. The *Asia Global* court considered the first four factors and recognized enforcement as a factor to be considered, but the evidence was equivocal regarding the existence or notice of corporate policies banning certain uses or monitoring of emails. Although *Asia Global* was not binding on the *Curto* court, it used it as further support for the consideration of the additional factor in the privilege analysis. *Curto*, 2006 WL 1318387, at *7–8.

enforcement of its computer usage policy created a "false sense of security" which "'lull[ed]' employees into believing that the policy would not be enforced."[212] In this sense, the fifth factor works as an additional safeguard to protect employees' privacy, because even if there is a monitoring policy in effect, it must further be determined if that policy is actually being enforced. Based on these findings, the court upheld a ruling that the plaintiff had not waived her right to assert the attorney-client privilege.[213]

Thus, the *Curto* case implemented a new factor in the traditional analysis of when inadvertent disclosure constitutes a waiver of the attorney-client privilege, which serves to protect the employees' privacy of personal communications with attorneys from a work computer.[214] Other courts could follow this approach and consider whether the employer in question actually enforced a monitoring policy in determining whether there was a waiver of the privilege. This would have the effect of giving the employee increased privacy rights when dealing with private communications to their attorneys that occur on employer-owned computers because, if an employee believed that her communications would remain confidential, the mere existence of a computer-monitoring policy would not be sufficient to destroy the privilege. It would further have to be shown that the employer actually *enforced* such a policy before there could be a waiver of the attorney-client privilege.[215]

2. *Legislative Solutions*

As an alternative to judicially-created methods to increase employee privacy protection for confidential communications with attorneys, both state and federal lawmakers could attempt to deal with the problem through legislation. On the federal side, an amendment to the ECPA may be helpful. At the state level, states could follow lead of New York and California to enact state legislation to increase the privacy rights of employees in this unique situation.

---

[212] *Id.* at *3. The lower court further found that there were only four instances in which the employer-defendant "monitored the computer use of its employees and that they occurred under very limited circumstances," such as "when there was a request by either a manager or supervisor or by someone else." *Id.*

[213] *Id.* at *9 (upholding the lower court's order finding that the plaintiff did not waive her attorney-client privilege).

[214] *See id.* at *8–9.

[215] *See id.* at *5.

a. *Amendment to the ECPA*

The ECPA makes the interception of an e-mail message by a third party a criminal act and protects the attorney-client privilege afforded any illegally intercepted message.[216] However, as discussed earlier,[217] workplace monitoring often falls under an exception to the statute because when an employee signs an employment agreement that allows his or her employer to monitor e-mail on employer-owned equipment, the employee gives up the statutory privacy protection afforded him by the ECPA.[218]

To increase employee privacy with respect to personal communications between the employee and his or her attorney, Congress could amend the ECPA to increase the protection given to privileged communications in monitored e-mail.[219] Under the current version of the ECPA, the statute only protects employees from someone intercepting their e-mail without their agreement and when employers are not monitoring during the "ordinary course of business."[220] To protect the privilege, the ECPA could be amended to provide absolute immunity from a waiver of the privilege so that an employee's consent under the statute to allow employer computer monitoring would not waive the privilege. In effect, for electronic communications qualifying as attorney-client privilege, the amendment would continue to regard employer interceptions of such communications "in accordance with" or "in violation of" the provisions of the statute, and thus the communications would not lose their privileged character.[221]

With such an amendment, employers who monitor employees' e-mail for "legitimate business purposes" would be prohibited from releasing e-mail between employees and their private attorneys, but the amendment would still allow employers to monitor the Internet activities of their employees in search of evidence of theft or other legitimate employee misbehavior. This amendment would serve both the legitimate business purpose that employers

---

[216] *See* 18 U.S.C. § 2511(1)(a) and (d) (2000). *See also* 18 U.S.C. § 2517(4) (2000) ("No otherwise privileged . . . electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.").

[217] *See supra* Part III.C.1.

[218] *See* Messer, *supra* note 24, at 92. Under these circumstances, employer interception of the e-mail is no longer "in accordance with" or "in violation of" the ECPA and loses the immunity from discovery afforded by § 2517(4). *Id.*

[219] *See* Messer, *supra* note 24, at 96.

[220] The case law discussed in the Messer note "indicates that courts are giving 'ordinary course of business' a very broad interpretation. As a result, the ECPA probably does not protect any employees in workplace monitoring situations." Messer, *supra* note 24, at 99 n.175.

[221] *See* 18 U.S.C. § 2517(4) (1994).

need to fulfill by monitoring e-mail while simultaneously protecting employees' privileged communications with their private attorneys.[222]

If Congress were to enact this change, even if an employee agrees to e-mail and monitoring as a condition of employment or use of his employer's computer system, the amendment would protect the confidentiality of his e-mail.[223] Although it is unclear how receptive Congress may be to this proposed change, it certainly would increase protection for employee's private e-mails to their attorneys, even if they had agreed to their employer's monitoring for business-related purposes.

b. *State Legislation*

The prevailing view of various bar associations is that although e-mail communication, like any other form of communication, carries the risk of unauthorized disclosure, lawyers and clients may communicate confidential information through unencrypted e-mail with a reasonable expectation of confidentiality and privacy.[224] Consistent with this trend, New York and California have enacted laws that provide some protection to e-mail communications. The New York law states that a privileged communication between an attorney and client does not lose its privileged character for the sole reason that it was sent by e-mail or because persons necessary for the

---

[222] *See* HÉBERT, *supra* note 14, § 8A, at 2.

[223] Messer, *supra* note 24, at 97. The author notes, however, that it is unlikely that "a business-friendly Congress will make such a trespass on the rights of most employers," as employer monitoring of computer usage is widespread in today's business world. *Id.* (citing a study revealing that more than fifty percent of over 1000 companies surveyed monitor employee e-mail).

[224] *E.g.*, ABCNY Comm. on Prof'l & Jud. Ethics, Formal Op. # 2000-1 (2000); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999), *available at* http://www.abanet.org/cpr/fo99-413.html; NYSBA Comm. on Prof'l Ethics, Op. 709, 1998 WL 957924 (1998). In addition, several state ethics committees have also approved the use of e-mail to transmit confidential communication. *See, e.g.*, D.C. Legal Ethics Comm. Op. 281 (1998), *available at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/281.cfm (no per se rule barring use of unencrypted Internet e-mail to transmit client confidences); S.C. Ethics Advisory Comm. Op. 281 (1998), *available at* http://www.scbar.org/member/opinion.asp?opinionID=469 (examining the privacy of Internet communications in view of current technology and laws prohibiting interception or monitoring of e-mail communications, and concluding that Internet users may have a reasonable expectation of confidentiality); VBA Advisory Ethics Op. 97-5(1997), *available at* https://www.vtbar.org/intus/cms/Display_Page.asp?PageID=5 (follow "Advisory Ethic Opinions" hyperlink, then follow "Confidences of the Client—Disclosure" hyperlink, then follow "97-05" hyperlink) (e-mail may pose no risk to confidentiality).

delivery or facilitation of the e-mail may have access to its content.[225] The California Evidence Code provides for a similar rule.[226] Thus, although there is disagreement,[227] these statutes provide that the transmission of a privileged communication thorough unencrypted e-mail does not, without more, destroy the privilege.

To expand the rights of employee privacy with respect to confidential communications with their lawyers, other states could follow the lead of New York and California and enact legislation specifically recognizing that the transmission of privileged communication through e-mail does not automatically destroy the privilege.[228] Moreover, states could expand even further to protect the attorney-client privilege by enacting specific statutes to protect e-mail communications in the unique situation in which an employee e-mails his attorney from an employer-owned computer. For example, the California statute could be amended to specifically provide protection of privileged information not only where a person involved in the "delivery, facilitation, or storage of electronic communication may have access to the content of the communication,"[229] but also where the employer actively monitors Internet use for business-related purposes. If this amendment was to be enacted and other states followed this lead, this is another possible way in which employee privacy could be enhanced.

This option—states adopting statutes similar to New York and California, or states further extending privacy to employees to cover the situation where an employee e-mails his private attorney from an employer-monitored computer—would be a step in the right direction for protecting employees' privileged communications with their attorneys on work computers. It would again preserve employers' legitimate business need to

---

[225] N.Y. C. P. L. R. § 4548 (McKinney 1999).

[226] CAL. EVID. CODE § 917(b) (West 2007) ("A communication between persons in [the attorney-client relationship] does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication.").

[227] *See, e.g.*, NYSBA Comm. on Prof'l Ethics, Op. 709 (1998), 1998 WL 957924, at *3 (finding that some ethics committees have not clearly approved the use of e-mail for confidential communications); Az. Op. 97-04 (e-mail may pose a risk to confidentiality); Iowa Sup. Ct. Bd. Of Prof'l Ethics & Conduct Op. 96-1 (1996), *available at* http://www.iowabar.org/ethics.nsf (follow "Iowa Board of Professional Ethics Opinions" hyperlink, then select Opinion 96-01 by following "08/29/1996" hyperlink) (attorneys must obtain waiver from clients as to e-mail security risk).

[228] *See, e.g.*, N.Y. C.P.F.R. § 4548 (McKinney 1999); CAL. EVID. CODE § 917(b) (West 2007).

[229] CAL. EVID. CODE § 917(b) (West 2007).

monitor employee Internet use, while also allowing employees to retain their privacy with respect to matters that do not pertain to their work.

3. *Requirement of Precaution by Attorneys*

In 1999, the ABA issued an opinion taking the position that sending confidential information through e-mail is no more a violation of the attorney-client privilege than making a telephone call or sending a facsimile, and it is not necessary for attorneys to take measures to secure their communications through encryption or other protective technologies.[230] In efforts to make employees more aware of the potential risk of communicating with their attorneys over e-mail in the workplace, it has been suggested that "[t]he ABA could issue a revised opinion on attorney-client e-mail communications."[231] The revised opinion could require that "an attorney warn his client of the risks inherent with confidential e-mail communications and [prohibit] confidential e-mail transmissions to and from a client's employer e-mail address." Under this opinion, "[w]hile clients might still access their personal e-mail from their employers' computers, they would do so knowing that they might be [putting the confidentiality in jeopardy or] waiving the privilege."[232] Given this warning, it is possible that clients "would find alternate ways of accessing their personal e-mail from their workplace that their employer cannot legally monitor, such as from their personal cell phones, pagers, or PDAs."[233]

The value of the ABA issuing a requirement of precaution by attorneys would provide enhanced protection to the attorney-client privilege in a relatively easy and cost-effective manner. Although the proponent of the opinion has noted possible burdens this may place on attorneys,[234] if the proposed opinion was merely revised to require an attorney to warn his client

---

[230] *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413, at Intro (1999), *available at* http://www.abanet.org/cpr/fo99-413.html.

[231] *See* Messer, *supra* note 24, at 97.

[232] *Id.* Messer notes that informing the client of the risk that the client might waive the "privilege would protect the attorney in any subsequent related malpractice actions" by the client. *Id.* at 98.

[233] *Id.*

[234] Messer discusses three burdens that attorneys would face under this approach. First, attorneys would have to learn to recognize employer e-mail addresses and refuse to use them. Second, attorneys would also have to warn their clients about the potential risks of workplace monitoring. Third, since some clients have only their employer e-mail addresses, attorneys would have to know where to direct their clients to get secure personal e-mail addresses. *Id.* However, in this author's opinion, the burden placed on attorneys is minimal compared to the value of the enhanced protection it would bring to the attorney-client privilege.

of the risks inherent with confidential communications being sent via e-mail, this would seem to place an extremely minimal burden on attorneys.[235] In fact, this approach can be harmonized with the ABA Model Rules and does not appear to overburden attorneys by requiring them to exercise precaution to simply advise their clients of the dangers that may exist.[236]

Therefore, it seems feasible that the ABA could issue an opinion containing general practice pointers and recommend that attorneys follow certain precautions when communicating with a client over e-mail. One author suggests that as workplace monitoring of employee computer use increases,[237] attorneys should exercise additional caution when communicating with clients, particularly when clients use an employer-issued computer to e-mail or prepare documents for their attorney.[238] The attorney should investigate whether the client is subject to computer monitoring, as the existence of employee monitoring should alert attorneys to a potential waiver of the attorney-client privilege and provide notice to the attorney that confidentiality dangers may arise. Attorneys should also consider the employee's awareness and consent to workplace monitoring.[239] Attorneys should look to the employer-employee agreement regarding computer use to assess whether the employee has a reasonable expectation of privacy,[240] and in accordance with the current case law, they should take note

---

[235] This approach would effectively eliminate the first and third burdens on attorneys, and the only duty the attorney would have would be to warn their clients about the potential risks of workplace monitoring.

[236] *See* MODEL RULES OF PROF'L CONDUCT R. 1.4 (2004). This approach is consistent with the Model Rules of Professional Conduct in several ways. Rule 1.4 governs communication, and it requires that a lawyer shall "reasonably consult with the client about the means by which the client's objectives are to be accomplished" as well as "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." *Id.* Thus, requiring a lawyer to advise his or her client of the possible dangers of communicating via e-mail from a work computer would constitute "consulting with the client about the means by which the client's objectives are to be accomplished," as well as explaining this circumstance of representation "to the extent reasonably necessary to permit the client to make informed decisions regarding the representation," in accordance with the ABA's requirements under the Model Rules. *See id.*

[237] *See supra* Part I for a discussion on the great increase of employer monitoring of employees.

[238] *See supra* Part I.

[239] *See supra* Part I.

[240] The attorney could also make suggestions as to how the employee can increase his expectation of privacy, such as suggesting that password-protection may serve to increase expectations of privacy.

that courts may also consider the enforcement, or lack of enforcement, of the policy.[241]

Employees may not be aware of the dangerous effect workplace monitoring can have on their confidential communications with their attorneys. The ABA can easily provide this knowledge to attorneys by issuing a revised opinion concerning computer usage. In turn, requiring attorneys to take these additional precautions to help make their clients aware of the potential dangers of e-mail communications appears to be a feasible option, consistent with other professional obligations,[242] to enhance employees' knowledge of privacy issues that may arise in the workplace.

VI. CONCLUSION

Given the tension between employers' legitimate need to monitor employees and the importance of both employee privacy and the attorney-client privilege, where does this leave Ashlee, our sexually harassed employee, who thought her communication was protected by the attorney-client privilege?

Courts have come out various ways on traditional privacy rights claims, and the recent cases involving the attorney-client privilege appear to be gathering mixed results as well. However, if the approach suggested in this Note is followed, Ashlee may be able to count on her attorney-client privilege after all. The court hearing Ashlee's lawsuit could follow the *Curto* court's approach. Under the *Curto* analysis, the court would take into consideration that Ashlee's employer did not enforce its monitoring policy and thus find that Ashlee had a reasonable expectation of privacy in her e-mail communications. Alternatively, federal and state legislatures could enact statutes to protect the privacy of others similarly situated to Ashlee. Or perhaps Ashlee's attorney should have been required to inform Ashlee of the possibility that e-mailing from a work computer where there is a computer monitoring policy may constitute a waiver of the attorney-client privilege. In this case, she may have been more precautious before e-mailing her attorney from work. If any of these approaches are followed, it is likely that Ashlee would be able to successfully assert her attorney-client privilege and withhold the documents from discovery.

An employee communicating with his or her attorney from a work computer presents a different problem than a traditional Fourth Amendment or common law invasion of privacy claim. This different context should be

---

[241] *See* Curto v. Medical World Communications, Inc., No. 03CV6327(DRH) (MLO), 2006 WL 1318387, at *4 (E.D.N.Y. May 15, 2006) ("Enforcement is a [r]elevant [c]onsideration.").

[242] *See* MODEL RULES OF PROF'L CONDUCT R. 1.4 (2004).

considered significant, and courts should follow the *Curto* court and find that they are not bound by the traditional expectation of privacy cases in this unique context. Given the importance of the attorney-client privilege and the changing technological landscape of modern businesses, courts, legislatures, and legal scholars should consider enacting stronger protections for employees who may find themselves in Ashlee's situation. As technology continues to expand and employees are working from around the globe, it seems only more likely that the problem Ashlee experienced will continue to increase. By adhering to any of the proposed solutions in this Note, employees' rights to privacy and attorney-client privilege can be protected, even in the face of our current "technological revolution," where computers are abundant and communication through e-mail is deemed almost necessary.